

Audit Report

Site report for CREG_AV

Audited on November 26, 2020

Reported on November 27, 2020

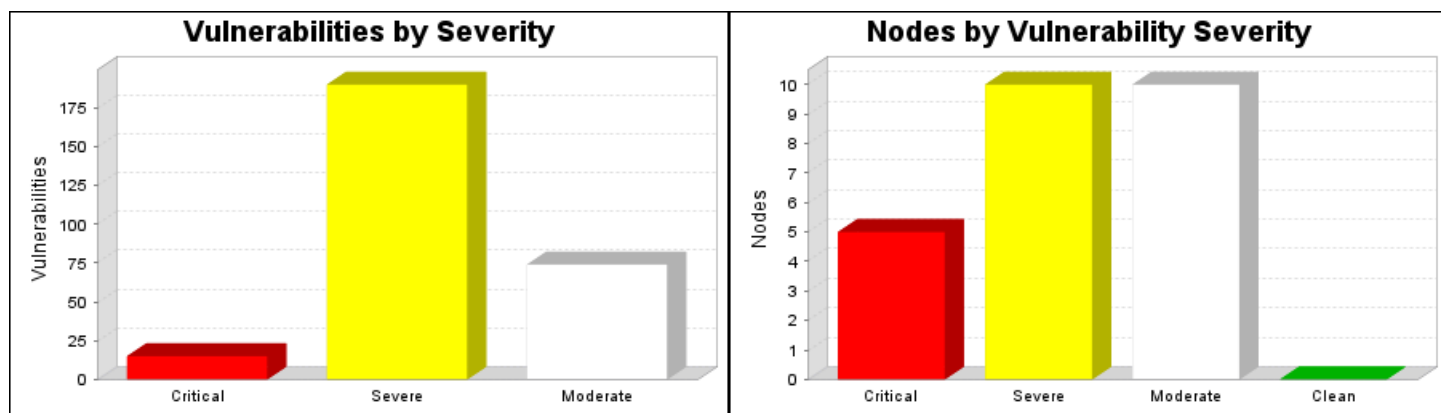
1. Executive Summary

This report represents a security audit performed by Nexpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

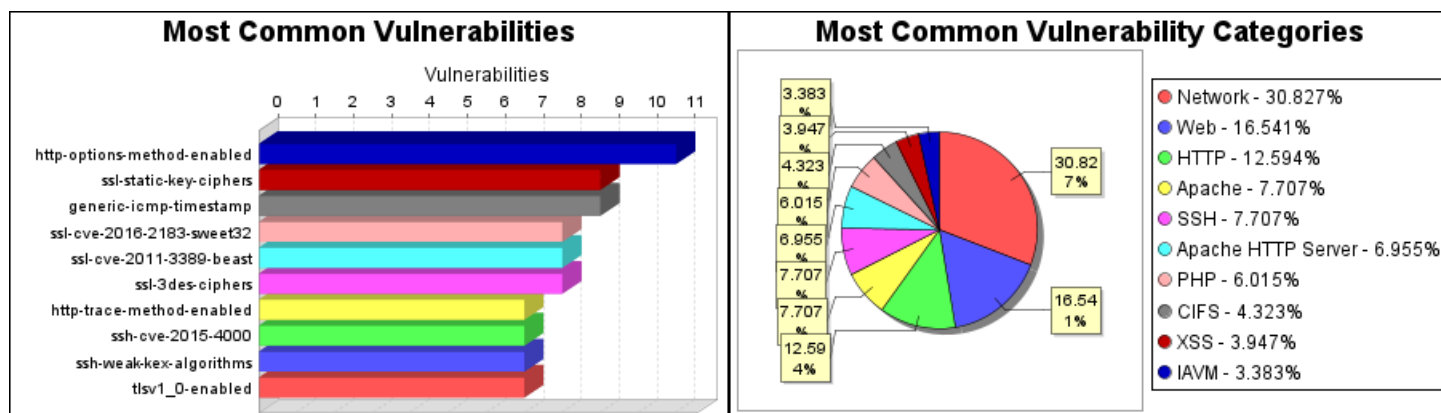
Site Name	Start Time	End Time	Total Time	Status
CREG_AV	November 26, 2020 00:52, COT	November 26, 2020 01:22, COT	30 minutes	Success

There is not enough historical data to display overall asset trend.

The audit was performed on 10 systems, 10 of which were found to be active and were scanned.



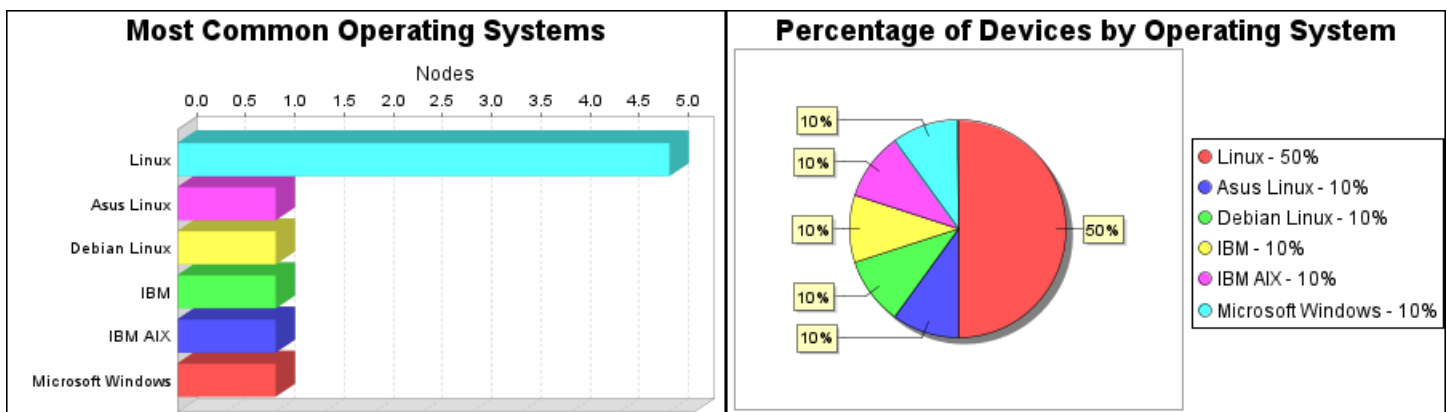
There were 279 vulnerabilities found during this scan. Of these, 15 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 190 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 74 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities. Critical vulnerabilities were found to exist on 5 of the systems, making them most susceptible to attack. 10 systems were found to have severe vulnerabilities. Moderate vulnerabilities were found on 10 systems. No systems were free of vulnerabilities.



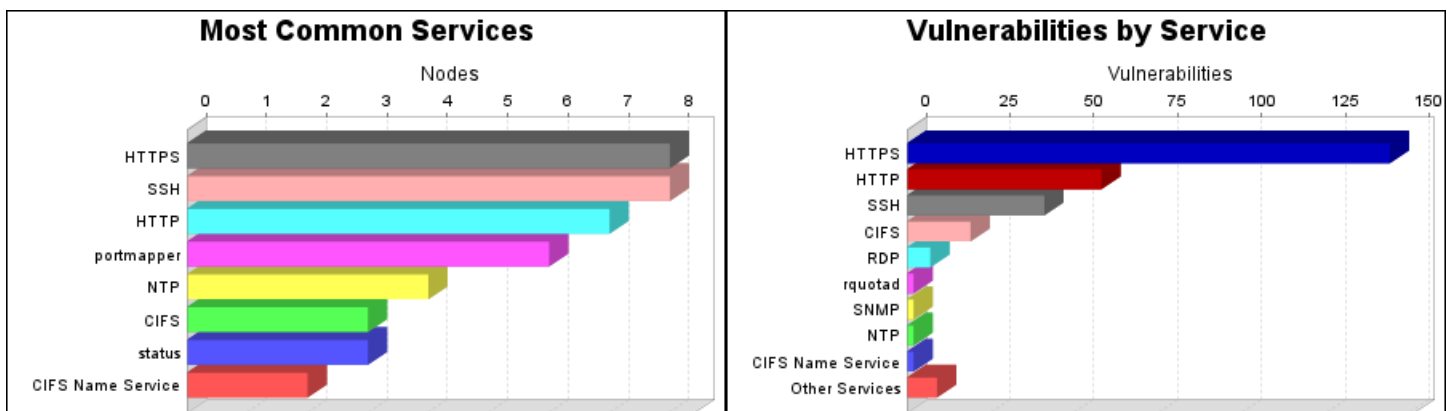
There were 11 occurrences of the http-options-method-enabled vulnerability, making it the most common vulnerability. There were 164 vulnerability instances in the Network category, making it the most common vulnerability category.



The http-options-method-enabled vulnerability poses the highest risk to the organization with a risk score of 6,296. Risk scores are based on the types and numbers of vulnerabilities on affected assets. There were 6 operating systems identified during this scan.



The Linux operating system was found on 5 systems, making it the most common operating system. There were 41 services found to be running during this scan.



The HTTPS and SSH services were found on 8 systems, making them the most common services. The HTTPS service was found to have the most vulnerabilities during this scan with 144 vulnerabilities.

2. Discovered Systems

Node	Operating System	Risk	Aliases
172.16.1.7	Linux 2.6.18	21,465	<ul style="list-style-type: none"> •CREGAS •cregas.creg.gov.co •cregas.creg.net
172.16.1.1	Linux 4.4	19,021	<ul style="list-style-type: none"> •cregweb.creg.gov.co •nuevo-portal.creg.net •www.creg.gov.co
172.16.1.180	Debian Linux	15,618	<ul style="list-style-type: none"> •DEBIAN •perseo.creg.gov.co •perseo.creg.net
172.16.1.46	IBM AIX 5.3	15,170	<ul style="list-style-type: none"> •zeus.creg.net
172.16.1.12	IBM AIX 6.1	14,750	<ul style="list-style-type: none"> •cregbd •cregbd.creg.gov.co •cregbd.creg.net
172.16.1.25	Linux 2.6.32	9,692	<ul style="list-style-type: none"> •utp.creg.net
172.16.1.156	Microsoft Windows Server 2012 R2 Datacenter Edition	8,969	<ul style="list-style-type: none"> •GESTORNORMATIVO •gestornormativo.creg.net
181.118.158.2	Asus Linux 2.6	3,140	
172.16.1.111	Linux 4.4	2,167	
172.16.1.103	Linux 4.4	1,590	<ul style="list-style-type: none"> •cregas-2018.creg.net

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

3.1.1. Default or Guessable SNMP community names: public (snmp-read-0001)

Description:

The Simple Network Management Protocol (SNMP) is a commonly used network service. Its primary function is to provide network administrators with information about all kinds of network connected devices. SNMP can be used to get and change system settings on a wide variety of devices, from network servers, to routers and printers. The drawback to this service is the authentication is an unencrypted "community string". In addition many SNMP servers provide very simple default community strings. The community string "public" is a default on a number of SNMP servers.

This community string can allow attackers to gain a large amount of information about the SNMP server and the network it monitors. Attackers may even reconfigure or shut down devices remotely.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:161	Running SNMP serviceSuccessfully authenticated to the SNMP service with credentials: uid[] pw[public] realm[]

References:

Source	Reference
BID	2896
BID	3795
BID	3797
CVE	CVE-1999-0186
CVE	CVE-1999-0254
CVE	CVE-1999-0472
CVE	CVE-1999-0516
CVE	CVE-1999-0517
CVE	CVE-2001-0514
CVE	CVE-2002-0109
CVE	CVE-2010-1574
XF	6576

Source	Reference
XF	7827

Vulnerability Solution:

•Secure the SNMP installation

1. If you do not absolutely need SNMP, disable it. SNMP versions 1 and 2c are inherently insecure. SNMP version 3 provides more complex authentication and encryption.
2. If you must use SNMP be sure to use complex and difficult to guess community names. Use the same policy for community names as you use for passwords.
3. Try to make all your MIB's read only. This will limit the damage an attacker can do to your network.

•Secure the SNMP installation on Cisco IOS

1. For SNMP Servers running on Cisco IOS, a Cisco IOS Software upgrade should be performed as a permanent fix for this vulnerability.
2. Alternatively, create an Embedded Event Manager policy to remove the hard-coded SNMP community names using the following steps:
3. event manager applet cisco-sa-20100707-snmp
4. event timer countdown time 30
5. action 10 cli command "enable"
6. action 20 cli command "configure terminal"
7. action 30 cli command "no snmp-server community public RO"
8. action 40 cli command "no snmp-server community private RW"
9. action 50 cli command "end"
10. action 60 cli command "disable"
11. action 70 syslog msg "Hard-coded SNMP community names as per Cisco Security Advisory cisco-sa-20100707-snmp removed"

<https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20100707-snmp.html>

3.1.2. 'rexec' Remote Execution Service Enabled (service-rexec)*Description:*

The RSH remote execution service (rexec) is enabled. This is a legacy service often configured to blindly trust some hosts and IPs. The protocol also doesn't support encryption or any sort of strong authentication mechanism.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:512	Running Remote Execution service

References:

None

Vulnerability Solution:

Disable or firewall this service which usually runs on 512/tcp.

3.1.3. Apache HTTPD: ap_get_basic_auth_pw() Authentication Bypass (CVE-2017-3167) (apache-httpd-cve-2017-3167)*Description:*

Use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed. Third-party module writers SHOULD use ap_get_basic_auth_components(), available in 2.2.34 and 2.4.26, instead of ap_get_basic_auth_pw(). Modules which call the legacy ap_get_basic_auth_pw() during the authentication phase MUST either immediately authenticate the user after the call, or else stop the request immediately with an error response, to avoid incorrectly authenticating the current request.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	99135
CVE	CVE-2017-3167
DEBIAN	DSA-3896
REDHAT	RHSA-2017:2478
REDHAT	RHSA-2017:2479
REDHAT	RHSA-2017:2483
REDHAT	RHSA-2017:3193
REDHAT	RHSA-2017:3194
REDHAT	RHSA-2017:3195
REDHAT	RHSA-2017:3475
REDHAT	RHSA-2017:3476
REDHAT	RHSA-2017:3477
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.34

Upgrade to Apache HTTPD version 2.2.34

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.34.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.26

Upgrade to Apache HTTPD version 2.4.26

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.26.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.1.4. Apache HTTPD: mod_ssl Null Pointer Dereference (CVE-2017-3169) (apache-httpd-cve-2017-3169)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_ssl. Review your web server configuration for validation. mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	99134
CVE	CVE-2017-3169
DEBIAN	DSA-3896
REDHAT	RHSA-2017:2478
REDHAT	RHSA-2017:2479
REDHAT	RHSA-2017:2483
REDHAT	RHSA-2017:3193
REDHAT	RHSA-2017:3194
REDHAT	RHSA-2017:3195
REDHAT	RHSA-2017:3475
REDHAT	RHSA-2017:3476
REDHAT	RHSA-2017:3477

Source	Reference
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

- Apache HTTPD >= 2.2 and < 2.2.34

Upgrade to Apache HTTPD version 2.2.34

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.34.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

- Apache HTTPD >= 2.4 and < 2.4.26

Upgrade to Apache HTTPD version 2.4.26

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.26.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.1.5. Apache HTTPD: mod_mime Buffer Overread (CVE-2017-7679) (apache-httpd-cve-2017-7679)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_mime. Review your web server configuration for validation. mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	99170
CVE	CVE-2017-7679
DEBIAN	DSA-3896
REDHAT	RHSA-2017:2478
REDHAT	RHSA-2017:2479
REDHAT	RHSA-2017:2483

Source	Reference
REDHAT	RHSA-2017:3193
REDHAT	RHSA-2017:3194
REDHAT	RHSA-2017:3195
REDHAT	RHSA-2017:3475
REDHAT	RHSA-2017:3476
REDHAT	RHSA-2017:3477
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

- Apache HTTPD >= 2.2 and < 2.2.34

Upgrade to Apache HTTPD version 2.2.34

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.34.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

- Apache HTTPD >= 2.4 and < 2.4.26

Upgrade to Apache HTTPD version 2.4.26

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.26.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.1.6. Apache Tomcat Example Scripts Information Leakage (apache-tomcat-example-leaks)

Description:

The following example scripts that come with Apache Tomcat v4.x - v7.x and can be used by attackers to gain information about the system. These scripts are also known to be vulnerable to cross site scripting (XSS) injection.

- /examples/jsp/num/numguess.jsp
- /examples/jsp/dates/date.jsp
- /examples/jsp/snp/snoop.jsp
- /examples/jsp/error/error.html
- /examples/jsp/sessions/carts.html
- /examples/jsp/checkbox/check.html
- /examples/jsp/colors/colors.html
- /examples/jsp/cal/login.html

- /examples/jsp/include/include.jsp
- /examples/jsp/forward/forward.jsp
- /examples/jsp/plugin/plugin.jsp
- /examples/jsp/jsptoserv/jsptoservlet.jsp
- /examples/jsp/simpletag/foo.jsp
- /examples/jsp/mail/sendmail.jsp
- /examples/servlet/HelloWorldExample
- /examples/servlet/RequestInfoExample
- /examples/servlet/RequestHeaderExample
- /examples/servlet/RequestParamExample
- /examples/servlet/CookieExample
- /examples/servlet/JndiServlet
- /examples/servlet/SessionExample
- /tomcat-docs/appdev/sample/web/hello.jsp

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.7:8080	<p>Running HTTP serviceProduct Tomcat exists -- Apache TomcatHTTP GET request to http://172.16.1.7:8080/tomcat-docs/appdev/sample/web/hello.jsp</p> <p>HTTP response code was an expected 200</p> <p>15: limitations under the License.</p> <p>16: --></p> <p>17: <html></p> <p>18: <head></p> <p>19: <title>Sample Application JSP Page</title></p>
172.16.1.7:8082	<p>Running HTTP serviceProduct Tomcat exists -- Apache TomcatHTTP GET request to http://172.16.1.7:8082/tomcat-docs/appdev/sample/web/hello.jsp</p> <p>HTTP response code was an expected 200</p> <p>15: limitations under the License.</p> <p>16: --></p> <p>17: <html></p> <p>18: <head></p> <p>19: <title>Sample Application JSP Page</title></p>

References:

None

Vulnerability Solution:

Delete these scripts entirely. Example scripts should never be installed on production servers.

3.1.7. Drupal: CVE-2019-11831: Drupal core - Moderately critical - Third-party libraries - SA-CORE-2019-007 (drupal-cve-2019-11831)

Description:

The PharStreamWrapper (aka phar-stream-wrapper) package 2.x before 2.1.1 and 3.x before 3.1.1 for TYPO3 does not prevent directory traversal, which allows attackers to bypass a deserialization protection mechanism, as demonstrated by a phar:///path/bad.phar/../../good.phar URL.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1	Vulnerable software installed: Drupal 7.60

References:

Source	Reference
BID	108302
CVE	CVE-2019-11831
DEBIAN	DSA-4445
URL	https://www.drupal.org/sa-core-2019-007

Vulnerability Solution:

- Upgrade to drupal version 7.67

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

- Upgrade to drupal version 8.6.1

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

- Upgrade to drupal version 8.7.1

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

3.1.8. Drupal: CVE-2019-6339: Drupal core - Critical - Arbitrary PHP code execution - SA-CORE-2019-002 (drupal-cve-2019-6339)

Description:

In Drupal Core versions 7.x prior to 7.62, 8.6.x prior to 8.6.6 and 8.5.x prior to 8.5.9; A remote code execution vulnerability exists in PHP's built-in phar stream wrapper when performing file operations on an untrusted phar:// URI. Some Drupal code (core, contrib, and custom) may be performing file operations on insufficiently validated user input, thereby being exposed to this vulnerability. This vulnerability is mitigated by the fact that such code paths typically require access to an administrative permission or an atypical configuration.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1	Vulnerable software installed: Drupal 7.60

References:

Source	Reference
CVE	CVE-2019-6339
DEBIAN	DSA-4370
URL	https://www.drupal.org/sa-core-2019-002

Vulnerability Solution:

- Upgrade to drupal version 7.62

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

- Upgrade to drupal version 8.5.9

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

- Upgrade to drupal version 8.6.6

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

3.1.9. Lotus Notes/Domino Anonymous Access to Domino Configuration Database (http-domino-0016)*Description:*

The Domino server has been configured to allow anonymous access to the Domino Configuration Database (domcfg.nsf). This database would allow an attacker to view and potentially modify URL mappings, URL redirection, and other administrative functions of your Domino site.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.46:80	Running HTTP serviceProduct Lotus Domino exists -- Lotus Domino 9.0.0.0 /domcfg.nsf

References:

None

Vulnerability Solution:

Open the database in the Lotus Notes client and edit the ACL.

Change the access level for Default and Anonymous to "No Access".

If this information is not critical for distribution to other domains, also restrict access for OtherDomainServers to "No Access".

For all entries set to "No Access", also verify that the "Read public documents" and "Write public documents" are unchecked. If not, access will still be permitted for any public documents.

3.1.10. OpenSSH X11 Cookie Local Authentication Bypass Vulnerability (openssh-x11-cookie-auth-bypass)

Description:

ssh in OpenSSH before 4.7 does not properly handle when an untrusted cookie cannot be created and uses a trusted X11 cookie instead, which allows attackers to violate intended policy and gain privileges by causing an X client to be treated as trusted.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.7:22	OpenBSD OpenSSH 4.3 on Linux 2.6.18

References:

Source	Reference
APPLE	APPLE-SA-2008-03-18
BID	25628
CVE	CVE-2007-4752
DEBIAN	DSA-1576
DISA_SEVERITY	Category II
DISA_VMSKEY	V0017144
IAVM	2008-T-0046
OVAL	10809
OVAL	5599
REDHAT	RHSA-2008:0855
XF	36637

Vulnerability Solution:

OpenBSD OpenSSH < 4.7

Download and apply the upgrade from: <ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH>

While you can always [build OpenSSH from source](#), many platforms and distributions provide pre-built binary packages for OpenSSH. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.1.11. PHP Vulnerability: CVE-2017-12932 (php-cve-2017-12932)*Description:*

ext/standard/var_unserializer.re in PHP 7.0.x through 7.0.22 and 7.1.x through 7.1.8 is prone to a heap use after free while unserializing untrusted data, related to improper use of the hash API for key deletion in a situation with an invalid array size. Exploitation of this issue can have an unspecified impact on the integrity of PHP.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
BID	100427
CVE	CVE-2017-12932
DEBIAN	DSA-4080
REDHAT	RHSA-2018:1296
REDHAT	RHSA-2019:2519
URL	https://bugs.php.net/bug.php?id=74103

Vulnerability Solution:

- Upgrade to PHP version 7.0.23
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.1.9
Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.12. PHP Vulnerability: CVE-2018-7584 (php-cve-2018-7584)*Description:*

In PHP through 5.6.33, 7.0.x before 7.0.28, 7.1.x through 7.1.14, and 7.2.x through 7.2.2, there is a stack-based buffer under-read while parsing an HTTP response in the `php_stream_url_wrap_http_ex` function in `ext/standard/http_fopen_wrapper.c`. This subsequently results in copying a large string.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
BID	103204
CVE	CVE-2018-7584
DEBIAN	DSA-4240

Source	Reference
REDHAT	RHSA-2019:2519

Vulnerability Solution:

- Upgrade to PHP version 5.6.34
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.0.28
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.1.15
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.3
Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.13. PHP Vulnerability: CVE-2019-9641 (php-cve-2019-9641)*Description:*

An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in `exif_process_IFD_in_TIFF`.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2019-9641
DEBIAN	DSA-4403
URL	https://bugs.php.net/bug.php?id=77509

Vulnerability Solution:

- Upgrade to PHP version 7.1.27
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.16
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.3.3
Download and apply the upgrade from: <http://www.php.net/releases/>

3.1.14. 'rsh' Remote Shell Service Enabled (service-rsh)

Description:

The RSH remote shell service (rsh) is enabled. This is a legacy service often configured to blindly trust some hosts and IPs. The protocol also doesn't support encryption or any sort of strong authentication mechanism.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:514	Running Remote Shell service

References:

Source	Reference
CVE	CVE-1999-0651

Vulnerability Solution:

Disable or firewall this service which usually runs on 514/tcp.

3.1.15. SNMP credentials transmitted in cleartext (snmp-cleartext-credential)*Description:*

The Simple Network Management Protocol (SNMP) is a commonly used network service. Its primary function is to provide network administrators with information about all kinds of network connected devices. SNMP can be used to get and change system settings on a wide variety of devices, from network servers, to routers and printers. The drawback to this service is the authentication is an unencrypted "community string". In addition many SNMP servers provide very simple default community strings.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:161	Successfully authenticated to the SNMP v1/v2c service.

References:

Source	Reference
CERT	CA-2002-03

Vulnerability Solution:

1. If you do not absolutely need SNMP, disable it. SNMP versions 1 and 2c are inherently insecure. SNMP version 3 provides more complex authentication and encryption.
2. If you must use SNMP be sure to use complex and difficult to guess community names. Use the same policy for community names as you use for passwords.
3. Try to make all your MIB's read only. This will limit the damage an attacker can do to your network.

3.2. Severe Vulnerabilities

3.2.1. Apache HTTPD: <FilesMatch> bypass with a trailing newline in the file name (CVE-2017-15715) (apache-httpd-cve-2017-15715)

Description:

The expression specified in <FilesMatch> could match '\$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are externally blocked, but only by matching the trailing portion of the filename.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	103525
CVE	CVE-2017-15715
DEBIAN	DSA-4164
REDHAT	RHSA-2018:3558
REDHAT	RHSA-2019:0366
REDHAT	RHSA-2019:0367
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.33

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.33.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.2. Apache HTTPD: Weak Digest auth nonce generation in mod_auth_digest (CVE-2018-1312) (apache-httpd-cve-2018-1312)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_auth_digest. Review your web server configuration for validation. When generating an HTTP Digest authentication challenge, the nonce sent to prevent replay attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication

configuration, HTTP requests could be replayed across servers by an attacker without detection.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	103524
CVE	CVE-2018-1312
DEBIAN	DSA-4164
REDHAT	RHSA-2018:3558
REDHAT	RHSA-2019:0366
REDHAT	RHSA-2019:0367
REDHAT	RHSA-2019:1898
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.33

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.33.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.3. X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)

Description:

The subject common name (CN) field in the X.509 certificate does not match the name of the entity presenting the certificate.

Before issuing a certificate, a Certification Authority (CA) must check the identity of the entity requesting the certificate, as specified in the CA's Certification Practice Statement (CPS). Thus, standard certificate validation procedures require the subject CN field of a certificate to match the actual name of the entity presenting the certificate. For example, in a certificate presented by "https://www.example.com/", the CN should be "www.example.com".

In order to detect and prevent active eavesdropping attacks, the validity of a certificate must be verified, or else an attacker could then launch a man-in-the-middle attack and gain full control of the data stream. Of particular importance is the validity of the subject's CN, that should match the name of the entity (hostname).

A CN mismatch most often occurs due to a configuration error, though it can also indicate that a man-in-the-middle attack is being conducted.

Please note that this check may flag a false positive against servers that are properly configured using SNI.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:443	The subject common name found in the X.509 certificate does not seem to match the scan target:Subject CN www.ibm.com does not match target name specified in the site.Subject CN www.ibm.com does not match DNS name specified in the site.Subject CN www.ibm.com does not match DNS name specified in the site.Subject CN resolved IP address differs from node IP address specified in the site.
172.16.1.156:443	The subject common name found in the X.509 certificate does not seem to match the scan target:Subject CN *.creg.gov.co does not match target name specified in the site.Subject CN *.creg.gov.co does not match DNS name specified in the site.Subject CN *.creg.gov.co could not be resolved to an IP address via DNS lookupSubject Alternative Name *.creg.gov.co does not match target name specified in the site.Subject Alternative Name creg.gov.co does not match target name specified in the site.Subject Alternative Name *.creg.gov.co does not match DNS name specified in the site.Subject Alternative Name creg.gov.co does not match DNS name specified in the site.
172.16.1.180:8181	The subject common name found in the X.509 certificate does not seem to match the scan target:Subject CN localhost does not match target name specified in the site.Subject CN localhost does not match DNS name specified in the site.Subject CN localhost does not match DNS name specified in the site. Subject CN resolved IP address differs from node IP address specified in the site.Subject CN resolved IP address differs from node IP address specified in the site.
172.16.1.25:8181	The subject common name found in the X.509 certificate does not seem to match the scan target:Subject CN creg.utp.edu.co does not match target name specified in the site.Subject CN creg.utp.edu.co does not match DNS name specified in the site.Subject CN resolved IP address differs from node IP address specified in the site.
172.16.1.46:5989	The subject common name found in the X.509 certificate does not seem to match the scan target:Subject CN PEGASUS TEST CERTIFICATE-DO NOT USE does not match target name specified in the site.Subject CN PEGASUS TEST CERTIFICATE-DO NOT USE does not match DNS name specified in the site.Subject CN PEGASUS TEST CERTIFICATE-DO NOT USE could not be resolved to an IP address via DNS lookup
181.118.158.2:8443	The subject common name found in the X.509 certificate does not seem to match the scan target:Subject CN FG3H1ETB18901831 does not match target name specified in the site.Subject CN FG3H1ETB18901831 could not be resolved to an IP address via DNS lookup

References:

None

Vulnerability Solution:

The subject's common name (CN) field in the X.509 certificate should be fixed to reflect the name of the entity presenting the certificate (e.g., the hostname). This is done by generating a new certificate usually signed by a Certification Authority (CA) trusted by both the client and server.

3.2.4. Weak LAN Manager hashing permitted (cifs-generic-0005)*Description:*

Microsoft are aware of detailed information and tools that might be used for attacks against NT LAN Manager version 1 (NTLMv1) and LAN Manager (LM) network authentication. Improvements in computer hardware and software algorithms have made these protocols vulnerable to published attacks for obtaining user credentials. The information and available toolsets specifically target environments that do not enforce NTLMv2 authentication. We strongly encourage customers to evaluate their environments and update network authentication settings. All supported Microsoft operating systems provide NTLMv2 authentication capabilities. Systems that are affected in a default configuration are primarily at risk, such as systems that are running Microsoft Windows NT 4, Windows 2000, Windows XP, and Windows Server 2003. For example, by default, Windows XP and Windows Server 2003 both support NTLMv1 authentication.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.25	Server did not return extended security data.
172.16.1.7	Server did not return extended security data.

References:

Source	Reference
URL	https://support.microsoft.com/en-us/help/2793313/security-guidance-for-ntlmv1-and-lm-network-authentication

Vulnerability Solution:

•Novell NetWare

Novell Network CIFS does not support NTLMv2

As of January 27, 2006 Novell Network CIFS does not support NTLMv2 authentication. [Click here](#) for more information.

•Microsoft

Upgrade the CIFS authentication method

Upgrade the authentication method using the registry. Note that upgrading the authentication method to NTLMv2 will break compatibility with Windows 95/98/ME systems and older pre-NT4 SP4 systems. This behavior is by design. If the system itself is NT4 SP3 or earlier, it must be upgraded to at least NT4 SP4 before making these changes. Note that the settings described below can also be set via Group Policy, under "Security Options", "LAN Manager Authentication Level".

Run the registry editor (regedit.exe or regedt32.exe) and browse to the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
and set the following value:

Value Name: LMCompatibilityLevel
Data Type: REG_DWORD
Data: Level 5 should be used.

The valid values are:

0	Send LM response and NTLM response; never use NTLMv2 session security
1	Use NTLMv2 session security if negotiated
2	Send NTLM authentication only
3	Send NTLMv2 authentication only
4	DC refuses LM authentication
5	DC refuses LM and NTLM authentication (accepts only NTLMv2)

You should also modify the following values to the highest levels:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\

Value Name: NtlmMinClientSec
Data Type: REG_DWORD
Data: See

[Security guidance for ntlmv1](https://support.microsoft.com/en-us/help/2793313/security-guidance-for-ntlmv1-and-lm-network-authentication) (<https://support.microsoft.com/en-us/help/2793313/security-guidance-for-ntlmv1-and-lm-network-authentication>) for details.

Value Name: NtlmMinServerSec
Data Type: REG_DWORD
Data: See

[Security guidance for ntlmv1](https://support.microsoft.com/en-us/help/2793313/security-guidance-for-ntlmv1-and-lm-network-authentication) (<https://support.microsoft.com/en-us/help/2793313/security-guidance-for-ntlmv1-and-lm-network-authentication>) for details.

You must then shut down and restart for the changes to take effect.

•Samba

Disable LANMAN Authentication In Samba

Add the following line in the smb.conf's global section:

lanman auth = No

3.2.5. SMB signing disabled (cifs-smb-signing-disabled)

Description:

This system does not allow SMB signing. SMB signing allows the recipient of SMB packets to confirm their authenticity and helps prevent man in the middle attacks against SMB. SMB signing can be configured in one of three ways: disabled entirely (least secure), enabled, and required (most secure).

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.156:139	SMB signing is disabled
172.16.1.156:445	SMB signing is disabled
172.16.1.25:139	SMB signing is disabled
172.16.1.25:445	SMB signing is disabled
172.16.1.7:139	SMB signing is disabled
172.16.1.7:445	SMB signing is disabled

References:

Source	Reference
URL	http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx

Vulnerability Solution:

•Microsoft Windows

Configure SMB signing for Windows

Configure the system to enable or require SMB signing as appropriate. The method and effect of doing this is system specific so please see [this TechNet article](#) for details. Note: ensure that SMB signing configuration is done for incoming connections (Server).

•Samba

Configure SMB signing for Samba

Configure Samba to enable or require SMB signing as appropriate. To enable SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:

```
server signing = auto
```

To require SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:

```
server signing = mandatory
```

3.2.6. Drupal: CVE-2018-1000888: Drupal core - Critical - Third Party Libraries - SA-CORE-2019-001 (drupal-cve-2018-1000888)

Description:

PEAR Archive_Tar version 1.4.3 and earlier contains a CWE-502, CWE-915 vulnerability in the Archive_Tar class. There are several file operations with ``$v_header['filename']`` as parameter (such as `file_exists`, `is_file`, `is_dir`, etc). When `extract` is called without a specific prefix path, we can trigger unserialization by crafting a tar file with ``phar://[path_to_malicious_phar_file]`` as path. Object injection can be used to trigger `destruct` in the loaded PHP classes, e.g. the `Archive_Tar` class itself. With `Archive_Tar` object injection, arbitrary file deletion can occur because ``@unlink($this->_temp_tarname)`` is called. If another class with useful gadget is loaded, it may possible to cause remote code execution that can result in files being deleted or possibly modified. This vulnerability appears to have been fixed in 1.4.4.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1	Vulnerable software installed: Drupal 7.60

References:

Source	Reference
CVE	CVE-2018-1000888
DEBIAN	DSA-4378
URL	https://www.drupal.org/sa-core-2019-001

Vulnerability Solution:

- Upgrade to drupal version 7.62
Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>
- Upgrade to drupal version 8.5.9
Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>
- Upgrade to drupal version 8.6.6
Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

3.2.7. PHP Vulnerability: CVE-2015-9253 (php-cve-2015-9253)*Description:*

An issue was discovered in PHP 7.3.x before 7.3.0alpha3, 7.2.x before 7.2.8, and before 7.1.20. The `php-fpm` master process restarts a child process in an endless loop when using program execution functions (e.g., `passthru`, `exec`, `shell_exec`, or `system`) with a non-blocking STDIN stream, causing this master process to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable

Affected Nodes:	Additional Information:
	version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2015-9253
URL	https://bugs.php.net/bug.php?id=70185
URL	https://bugs.php.net/bug.php?id=73342https://github.com/php/php-src/pull/3287
URL	https://bugs.php.net/bug.php?id=75968

Vulnerability Solution:

- Upgrade to PHP version 7.1.20

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.2.8

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.8. PHP Vulnerability: CVE-2018-10549 (php-cve-2018-10549)*Description:*

An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_iif_add_value mishandles the case of a MakerNote that lacks a final '\0' character.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
BID	104019
CVE	CVE-2018-10549
DEBIAN	DSA-4240
REDHAT	RHSA-2019:2519
URL	https://bugs.php.net/bug.php?id=76130

Vulnerability Solution:

- Upgrade to PHP version 5.6.36

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.0.30
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.1.17
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.5
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.9. POP credentials transmitted unencrypted (pop-plaintext-auth)

Description:

The server supports authentication methods where credentials are sent in plaintext over unencrypted channels. If an attacker can intercept traffic between a client and this server, the credentials would be exposed.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.46:110	Running POP serviceConfiguration item pop.plaintext.authentication set to 'true' matched

References:

None

Vulnerability Solution:

Follow the product-specific documentation to disable plaintext authentication methods for the POP service.

3.2.10. SMTP credentials transmitted unencrypted (smtp-plaintext-auth)

Description:

The server supports authentication methods where credentials are sent in plaintext over unencrypted channels. If an attacker can intercept traffic between a client and this server, the credentials would be exposed.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.46:25	Running SMTP serviceConfiguration item smtp.plaintext.authentication set to 'true' matched

References:

None

Vulnerability Solution:

Follow the product-specific documentation to disable plaintext authentication methods for the SMTP service.

3.2.11. X.509 Server Certificate Is Invalid/Expired (tls-server-cert-expired)

Description:

The TLS/SSL server's X.509 certificate either contains a start date in the future or is expired. Please refer to the proof for more details.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.46:5989	The certificate is not valid after Fri, 27 Mar 2015 02:49:19 COT
172.16.1.7:443	The certificate is not valid after Wed, 14 Nov 2007 16:51:08 COT

References:

None

Vulnerability Solution:

Obtain a new certificate and install it on the server. The exact instructions for obtaining a new certificate depend on your organization's requirements. Generally, you will need to generate a certificate request and save the request as a file. This file is then sent to a Certificate Authority (CA) for processing. Please ensure that the start date and the end date on the new certificate are valid.

Your organization may have its own internal Certificate Authority. If not, you may have to pay for a certificate from a trusted external Certificate Authority.

After you have received a new certificate file from the Certificate Authority, you will have to install it on the TLS/SSL server. The exact instructions for installing a certificate differ for each product. Please follow their documentation.

3.2.12. Apache HTTPD: Uninitialized memory reflection in mod_auth_digest (CVE-2017-9788) (apache-httpd-cve-2017-9788)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_auth_digest. Review your web server configuration for validation. The value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments. by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	99569
CVE	CVE-2017-9788
DEBIAN	DSA-3913
REDHAT	RHSA-2017:2478
REDHAT	RHSA-2017:2479
REDHAT	RHSA-2017:2483
REDHAT	RHSA-2017:2708
REDHAT	RHSA-2017:2709
REDHAT	RHSA-2017:2710
REDHAT	RHSA-2017:3113
REDHAT	RHSA-2017:3114
REDHAT	RHSA-2017:3193
REDHAT	RHSA-2017:3194
REDHAT	RHSA-2017:3195
REDHAT	RHSA-2017:3239
REDHAT	RHSA-2017:3240
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.34

Upgrade to Apache HTTPD version 2.2.34

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.34.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.27

Upgrade to Apache HTTPD version 2.4.27

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.27.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.13. Apache HTTPD: mod_auth_digest access control bypass (CVE-2019-0217) (apache-httpd-cve-2019-0217)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_auth_digest. Review your web server configuration for validation. In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	107668
CVE	CVE-2019-0217
DEBIAN	DSA-4422
REDHAT	RHSA-2019:2343
REDHAT	RHSA-2019:3436
REDHAT	RHSA-2019:3932
REDHAT	RHSA-2019:3933
REDHAT	RHSA-2019:3935
REDHAT	RHSA-2019:4126
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.39

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.39.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.14. Apache HTTPD: mod_rewrite potential open redirect (CVE-2019-10098) (apache-httpd-cve-2019-10098)*Description:*

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_rewrite. Review your web server configuration for validation. Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
CVE	CVE-2019-10098
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.41

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.41.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.15. Apache HTTPD: mod_rewrite CWE-601 open redirect (CVE-2020-1927) (apache-httpd-cve-2020-1927)*Description:*

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_rewrite. Review your web server configuration for validation. Apache HTTP Server versions 2.4.0 to 2.4.41 Some mod_rewrite configurations vulnerable to open redirect.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
CVE	CVE-2020-1927
DEBIAN	DSA-4757
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.42

Download and apply the upgrade from: <https://httpd.apache.org/download.cgi#apache24>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

operating system.

3.2.16. SMB signing not required (cifs-smb-signing-not-required)

Description:

This system enables, but does not require SMB signing. SMB signing allows the recipient of SMB packets to confirm their authenticity and helps prevent man in the middle attacks against SMB. SMB signing can be configured in one of three ways: disabled entirely (least secure), enabled, and required (most secure).

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.156:139	Smb signing is: disabled
172.16.1.156:445	Smb signing is: disabled
172.16.1.25:139	Smb signing is: disabled
172.16.1.25:445	Smb signing is: disabled
172.16.1.7:139	Smb signing is: disabled
172.16.1.7:445	Smb signing is: disabled

References:

Source	Reference
URL	http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx

Vulnerability Solution:

•Microsoft Windows

Configure SMB signing for Windows

Configure the system to enable or require SMB signing as appropriate. The method and effect of doing this is system specific so please see [this TechNet article](#) for details. Note: ensure that SMB signing configuration is done for incoming connections (Server).

•Samba

Configure SMB signing for Samba

Configure Samba to enable or require SMB signing as appropriate. To enable SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:

```
server signing = auto
```

To require SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:

```
server signing = mandatory
```

3.2.17. SMB: Service supports deprecated SMBv1 protocol (cifs-smb1-deprecated)

Description:

The SMB1 protocol has been deprecated since 2014 and is considered obsolete and insecure.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.156:139	SMB1 is deprecated and should not be used
172.16.1.156:445	SMB1 is deprecated and should not be used
172.16.1.25:139	SMB1 is deprecated and should not be used
172.16.1.25:445	SMB1 is deprecated and should not be used
172.16.1.7:139	SMB1 is deprecated and should not be used
172.16.1.7:445	SMB1 is deprecated and should not be used

References:

Source	Reference
URL	https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

Vulnerability Solution:

•Samba

Remove/disable SMB1

For Samba systems on Linux, disabling SMB1 is quite straightforward: _

[How to configure Samba to use SMBv2 and disable SMBv1 on Linux or Unix](#)

•Microsoft Windows

Remove/disable SMB1

For Windows 8.1 and Windows Server 2012 R2, removing SMB1 is trivial. On older OS'es it can't be removed but should be disabled.

This article contains system-specific details: _

[How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server](#)

3.2.18. SMBv2 signing not required (cifs-smb2-signing-not-required)

Description:

This system enables, but does not require SMB signing. SMB signing allows the recipient of SMB packets to confirm their authenticity and helps prevent man in the middle attacks against SMB. SMB 2.x signing can be configured in one of two ways: not required (least secure) and required (most secure).

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.156:445	Running CIFS serviceConfiguration item smb2-enabled set to 'true' matched Configuration item smb2-signing set to 'enabled' matched

References:

Source	Reference
URL	https://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx

Vulnerability Solution:

•Microsoft Windows

Configure SMB signing for Windows

Configure the system to enable or require SMB signing as appropriate. The method and effect of doing this is system specific so please see [this TechNet article](#) for details. Note: ensure that SMB signing configuration is done for incoming connections (Server).

•Samba

Configure SMB signing for Samba

Configure Samba to enable or require SMB signing as appropriate. To enable SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:

```
server signing = auto
```

To require SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:

```
server signing = mandatory
```

3.2.19. Drupal: CVE-2019-6338: Drupal core - Critical - Third Party Libraries - SA-CORE-2019-001 (drupal-cve-2019-6338)

Description:

In Drupal Core versions 7.x prior to 7.62, 8.6.x prior to 8.6.6 and 8.5.x prior to 8.5.9; Drupal core uses the third-party PEAR Archive_Tar library. This library has released a security update which impacts some Drupal configurations. Refer to CVE-2018-1000888 for details

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1	Vulnerable software installed: Drupal 7.60

References:

Source	Reference
BID	106706
CVE	CVE-2019-6338
DEBIAN	DSA-4370
URL	https://www.drupal.org/sa-core-2019-001

Vulnerability Solution:

- Upgrade to drupal version 7.62
Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>
- Upgrade to drupal version 8.5.9
Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>
- Upgrade to drupal version 8.6.6
Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

3.2.20. HTTP DELETE Method Enabled (http-delete-method-enabled)*Description:*

The Web server contains a flaw that may allow a remote attacker to delete arbitrary files by using the HTTP method 'DELETE', resulting in a loss of integrity.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:8080	DELETE method found via OPTIONS banner
172.16.1.180:8181	DELETE method found via OPTIONS banner
172.16.1.25:8181	DELETE method found via OPTIONS banner

References:

Source	Reference
OWASP-2010	A6
OWASP-2013	A5
OWASP-2013	A9

Source	Reference
XF	http-delete(4253)

Vulnerability Solution:

•Apache HTTPD

Disable HTTP DELETE Method for Apache

Disable the DELETE method by including the following in the Apache configuration:

```
<Limit DELETE>
```

```
Order deny,allow
```

```
Deny from all
```

```
</Limit>
```

•Java System Web Server, SunONE WebServer, Sun-ONE-Web-Server, iPlanet

Disable HTTP DELETE Method for Sun Java System Web Server (or Sun ONE Web Server, iPlanet Web Server, Netscape Enterprise Server)

In the server.xml configuration file, add the following lines to restrict the DELETE method to a particular user(s):

```
acl "uri=/dir/*";
```

```
deny(all)
```

```
user="anyone";
```

```
allow(read,list,execute,info)
```

```
user="all";
```

```
allow (read,list,execute,info,write,delete)
```

```
user = "username";
```

•Microsoft IIS

Disable HTTP DELETE Method for IIS

Disable the DELETE method by doing the following in the IIS manager

1. Select relevant site
2. Select Request filtering and change to HTTP verb tab
3. Select Deny Verb from the actions pane
4. Type DELETE into the provided text box and press OK

•nginx nginx

Disable HTTP DELETE Method for nginx

Disable the DELETE method by adding the following line to your server block in your config file, you can add other HTTP methods to be allowed to run after POST

```
limit_except GET POST { deny all; }
```

- Disable HTTP DELETE method

Disable HTTP DELETE method on your web server. Refer to your web server's instruction manual on how to do this.

Web servers that respond to the DELETE HTTP method expose what other methods are supported by the web server, allowing attackers to narrow and intensify their efforts.

3.2.21. HTTP TRACE Method Enabled (http-trace-method-enabled)

Description:

The HTTP TRACE method is normally used to return the full HTTP request back to the requesting client for proxy-debugging purposes. An attacker can create a webpage using XMLHTTP, ActiveX, or XMLHttpRequest to cause a client to issue a TRACE request and capture the client's cookies. This effectively results in a Cross-Site Scripting attack.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:80	Running HTTP serviceHTTP TRACE request to http://172.16.1.1/ 1: TRACE / HTTP/1.1 2: Host: 172.16.1.1 3: Cookie: vulnerable=yes
172.16.1.1:443	Running HTTPS serviceHTTP TRACE request to https://172.16.1.1/ 1: TRACE / HTTP/1.1 2: Host: 172.16.1.1 3: Cookie: vulnerable=yes
172.16.1.25:8181	Running HTTPS serviceHTTP TRACE request to https://172.16.1.25:8181/ 1: TRACE / HTTP/1.1 2: host: 172.16.1.25:8181 3: cookie: vulnerable=yes
172.16.1.46:80	Running HTTP serviceHTTP TRACE request to http://172.16.1.46/ 1: TRACE / HTTP/1.1 2: Host: 172.16.1.46 3: Cookie: vulnerable=yes
172.16.1.7:80	Running HTTP serviceHTTP TRACE request to http://172.16.1.7/ 1: TRACE / HTTP/1.1 2: Host: 172.16.1.7 3: Cookie: vulnerable=yes

Affected Nodes:	Additional Information:
172.16.1.7:443	Running HTTPS serviceHTTP TRACE request to https://172.16.1.7/ 1: TRACE / HTTP/1.1 2: Host: 172.16.1.7 3: Cookie: vulnerable=yes
172.16.1.7:7778	Running HTTP serviceHTTP TRACE request to http://172.16.1.7:7778/ 1: TRACE / HTTP/1.1 2: Host: 172.16.1.7:7778 3: Cookie: vulnerable=yes

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
BID	15222
BID	19915
BID	24456
BID	36956
BID	9506
CERT-VN	867593
CVE	CVE-2004-2320
CVE	CVE-2004-2763
CVE	CVE-2005-3398
CVE	CVE-2006-4683
CVE	CVE-2007-3008
CVE	CVE-2008-7253
CVE	CVE-2009-2823
CVE	CVE-2010-0386
DISA_SEVERITY	Category II
DISA_VMSKEY	V0011706
IAVM	2005-T-0043
OSVDB	35511
OSVDB	3726
OVAL	1445
URL	http://www.apacheweek.com/issues/03-01-24#news
URL	http://www.kb.cert.org/vuls/id/867593

Source	Reference
XF	14959
XF	34854

Vulnerability Solution:

•Apache HTTPD, Apache Tomcat

Disable HTTP TRACE Method for Apache

Newer versions of Apache (1.3.34 and 2.0.55 and later) provide a configuration directive called TraceEnable. To deny TRACE requests, add the following line to the server configuration:

TraceEnable off

For older versions of the Apache webserver, use the mod_rewrite module to deny the TRACE requests:

RewriteEngine On

RewriteCond %{REQUEST_METHOD} ^TRACE

RewriteRule .* - [F]

In Apache Tomcat, the HTTP Trace can be disabled by adding security constraints into the Java Servlet specification within the web.xml configuration file and by setting the attribute allowTrace="False" to the HTTP connector in server.xml. For Spring Boot embedded Tomcat configuration, please refer [here](#)

•IIS, PWS, Microsoft-IIS, Internet Information Services, Internet Information Services, Microsoft-PWS

Disable HTTP TRACE Method for Microsoft IIS

For Microsoft Internet Information Services (IIS), you may use the URLScan tool, freely available at <http://www.microsoft.com/technet/security/tools/urlscan.mspx>

•Java System Web Server, SunONE WebServer, Sun-ONE-Web-Server, iPlanet

Disable HTTP TRACE Method for SunONE/iPlanet

•For Sun ONE/iPlanet Web Server v6.0 SP2 and later, add the following configuration to the top of the default object in the 'obj.conf' file:

```
<Client method="TRACE">
```

```
AuthTrans fn="set-variable"
```

```
remove-headers="transfer-encoding"
```

```
set-headers="content-length: -1"
```

```
error="501"
```

```
</Client>
```

You must then restart the server for the changes to take effect.

•For Sun ONE/iPlanet Web Server prior to v6.0 SP2, follow the instructions provided the 'Relief/Workaround' section of Sun's official advisory: <http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603>

•Lotus Domino

Disable HTTP TRACE Method for Domino

Follow [IBM's instructions](#) for disabling HTTP methods on the Domino server by adding the following line to the server's NOTES.INI file: HTTPDisableMethods=TRACE

After saving NOTES.INI, restart the Notes web server by issuing the console command "tell http restart".

3.2.22. Lotus Notes Server Does Not Require Port Encryption (lotus-notes-port-encryption-not-required)

Description:

Lotus Notes and Domino servers support a proprietary protocol called NotesRPC, commonly known as the Notes protocol. This protocol allows the client and server to negotiate encryption of all network traffic. By default, port encryption is not enabled. This may expose sensitive data to malicious users capable of monitoring network traffic.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.46:1352	Server accepts unencrypted connections.

References:

None

Vulnerability Solution:

To enable port encryption on the server, the following steps can be used from the Lotus Notes administration client:

1. Select the server to be configured.
2. Click on the "Server" tab.
3. Click on the "Status" tab.
4. Expand the "Tools" option (on the right).
5. Expand the "Server" option.
6. Click on "Setup Ports...".
7. For each port, check the "Encrypt network data" checkbox then click OK.

The ports that were changed or the entire server must then be restarted for the changes to take effect.

3.2.23. PHP Vulnerability: CVE-2019-11034 (php-cve-2019-11034)

Description:

When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.28, 7.2.x below 7.2.17 and 7.3.x below 7.3.4 can be caused to read past allocated buffer in `exif_process_IFD_TAG` function. This may lead to information disclosure or crash.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference

Source	Reference
CVE	CVE-2019-11034
DEBIAN	DSA-4529
REDHAT	RHSA-2019:2519
REDHAT	RHSA-2019:3299
URL	https://bugs.php.net/bug.php?id=77753

Vulnerability Solution:

- Upgrade to PHP version 7.1.28
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.17
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.3.4
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.24. PHP Vulnerability: CVE-2019-11035 (php-cve-2019-11035)*Description:*

When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.28, 7.2.x below 7.2.17 and 7.3.x below 7.3.4 can be caused to read past allocated buffer in `exif_iif_add_value` function. This may lead to information disclosure or crash.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2019-11035
DEBIAN	DSA-4529
REDHAT	RHSA-2019:2519
REDHAT	RHSA-2019:3299
URL	https://bugs.php.net/bug.php?id=77831

Vulnerability Solution:

- Upgrade to PHP version 7.1.28
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.17
Download and apply the upgrade from: <http://www.php.net/releases/>

•Upgrade to PHP version 7.3.4

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.25. PHP Vulnerability: CVE-2019-11036 (php-cve-2019-11036)

Description:

When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.29, 7.2.x below 7.2.18 and 7.3.x below 7.3.5 can be caused to read past allocated buffer in exif_process_IFD_TAG function. This may lead to information disclosure or crash.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
BID	108177
CVE	CVE-2019-11036
DEBIAN	DSA-4527
DEBIAN	DSA-4529
REDHAT	RHSA-2019:2519
REDHAT	RHSA-2019:3299
URL	https://bugs.php.net/bug.php?id=77950

Vulnerability Solution:

•Upgrade to PHP version 7.1.29

Download and apply the upgrade from: <http://www.php.net/releases/>

•Upgrade to PHP version 7.2.18

Download and apply the upgrade from: <http://www.php.net/releases/>

•Upgrade to PHP version 7.3.5

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.26. PHP Vulnerability: CVE-2019-11039 (php-cve-2019-11039)

Description:

Function iconv_mime_decode_headers() in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 may perform out-of-buffer read due to integer overflow when parsing MIME headers. This may lead to information disclosure or crash.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2019-11039
DEBIAN	DSA-4527
DEBIAN	DSA-4529
REDHAT	RHSA-2019:2519
REDHAT	RHSA-2019:3299
URL	https://bugs.php.net/bug.php?id=78069

Vulnerability Solution:

- Upgrade to PHP version 7.1.30
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.19
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.3.6
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.27. PHP Vulnerability: CVE-2019-11040 (php-cve-2019-11040)*Description:*

When PHP EXIF extension is parsing EXIF information from an image, e.g. via `exif_read_data()` function, in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2019-11040

Source	Reference
DEBIAN	DSA-4527
DEBIAN	DSA-4529
REDHAT	RHSA-2019:2519
REDHAT	RHSA-2019:3299
URL	https://bugs.php.net/bug.php?id=77988

Vulnerability Solution:

- Upgrade to PHP version 7.1.30
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.19
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.3.6
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.28. PHP Vulnerability: CVE-2019-11041 (php-cve-2019-11041)*Description:*

When PHP EXIF extension is parsing EXIF information from an image, e.g. via `exif_read_data()` function, in PHP versions 7.1.x below 7.1.31, 7.2.x below 7.2.21 and 7.3.x below 7.3.8 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2019-11041
DEBIAN	DSA-4527
DEBIAN	DSA-4529
REDHAT	RHSA-2019:3299
URL	https://bugs.php.net/bug.php?id=78222

Vulnerability Solution:

- Upgrade to PHP version 7.1.31
Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.2.21

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.3.8

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.29. PHP Vulnerability: CVE-2019-11042 (php-cve-2019-11042)

Description:

When PHP EXIF extension is parsing EXIF information from an image, e.g. via `exif_read_data()` function, in PHP versions 7.1.x below 7.1.31, 7.2.x below 7.2.21 and 7.3.x below 7.3.8 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2019-11042
DEBIAN	DSA-4527
DEBIAN	DSA-4529
REDHAT	RHSA-2019:3299
URL	https://bugs.php.net/bug.php?id=78256

Vulnerability Solution:

- Upgrade to PHP version 7.1.31

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.2.21

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.3.8

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.30. TLS/SSL Server Supports DES and IDEA Cipher Suites (ssl-des-ciphers)

Description:

Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) include cipher suites based on the DES (Data Encryption Standard) and IDEA (International Data Encryption Algorithm) algorithms. DES and IDEA algorithms are no longer recommended for general use in TLS, and have been removed from TLS version 1.2.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DHE_RSA_WITH_DES_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA
172.16.1.46:5989	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_WITH_DES_CBC_SHA TLS 1.0 ciphers: TLS_RSA_WITH_DES_CBC_SHA
172.16.1.7:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DHE_RSA_WITH_DES_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA TLS 1.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DHE_RSA_WITH_DES_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA

References:

Source	Reference
URL	http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295
URL	https://wiki.mozilla.org/Security/Server_Side_TLS
URL	https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Rule_-_Only_Support_Strong_Cryptographic_Ciphers
URL	http://support.microsoft.com/kb/245030/
URL	https://tools.ietf.org/html/rfc5469

Vulnerability Solution:

Configure the server to disable support for DES and IDEA cipher suites.

For Microsoft IIS web servers, see Microsoft Knowledgebase article [245030](http://support.microsoft.com/kb/245030/) for instructions on disabling DES and IDEA cipher suites.

The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.

Refer to your server vendor documentation to apply the recommended cipher configuration:

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

3.2.31. TLS/SSL Server Supports Export Cipher Algorithms (ssl-export-ciphers)

Description:

The TLS/SSL server supports export cipher suites, intentionally crippled to conform to US export laws. Symmetric ciphers used in export cipher suites typically do not exceed 56 bits.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5
172.16.1.7:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5 TLS 1.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5

References:

Source	Reference
URL	http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295
URL	https://wiki.mozilla.org/Security/Server_Side_TLS
URL	https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Rule_-_Only_Support_Strong_Cryptographic_Ciphers
URL	http://support.microsoft.com/kb/245030/

Vulnerability Solution:

Configure the server to disable support for export ciphers.

For Microsoft IIS web servers, see Microsoft Knowledgebase article [245030](http://support.microsoft.com/kb/245030/) for instructions on disabling export ciphers.

The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.

Refer to your server vendor documentation to apply the recommended cipher configuration:

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-

SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

3.2.32. TLS/SSL Server Supports SSLv2 (ssl2-enabled)

Description:

The server accepts clients using SSLv2. SSLv2 is an older implementation of the Secure Sockets Layer protocol. It suffers from a number of security flaws allowing attackers to capture and alter information passed between a client and the server, including the following weaknesses:

- No protection from against man-in-the-middle attacks during the handshake.
- Weak MAC construction and MAC relying solely on the MD5 hash function.
- Exportable cipher suites unnecessarily weaken the MACs
- Same cryptographic keys used for message authentication and encryption.
- Vulnerable to truncation attacks by forged TCP FIN packets

SSLv2 has been deprecated and is no longer recommended. Note that neither SSLv2 nor SSLv3 meet the U.S. FIPS 140-2 standard, which governs cryptographic modules for use in federal information systems. Only the newer TLS (Transport Layer Security) protocol meets FIPS 140-2 requirements. In addition, the presence of an SSLv2-only service on a host is deemed a failure by the PCI (Payment Card Industry) Data Security Standard.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.7:443	Successfully connected over SSLv2

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/pdfs/pcissc_assessors_nl_2008-11.pdf
URL	https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

Vulnerability Solution:

•Apache HTTPD

Disable SSLv2 protocol support in Apache HTTPD

For Apache web servers with mod_ssl, edit the Apache configuration file and change the SSLCipherSuite line to read:

SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:!SSLv2

The ! (exclamation point) before SSLv2 is what disables this protocol.

•Windows

Disable SSLv2 protocol support in Microsoft Windows

Configure the server to require clients to use at least SSLv3 or TLS.

For Microsoft Windows before Windows 2003, see [KB187498](#). For newer versions of Microsoft Windows, see [KB245030](#).

•Disable insecure TLS/SSL protocol support

Configure the server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.

3.2.33. Untrusted TLS/SSL server X.509 certificate (tls-untrusted-ca)

Description:

The server's TLS/SSL certificate is signed by a Certification Authority (CA) that is not well-known or trusted. This could happen if: the chain/intermediate certificate is missing, expired or has been revoked; the server hostname does not match that configured in the certificate; the time/date is incorrect; or a self-signed certificate is being used. The use of a self-signed certificate is not recommended since it could indicate that a TLS/SSL man-in-the-middle attack is taking place

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:443	TLS/SSL certificate signed by unknown, untrusted CA: CN=www.ibm.com, OU=STG, O=IBM, L=Austin, ST=TX, C=US -- [Path does not chain with any of the trust anchors].
172.16.1.180:8181	TLS/SSL certificate signed by unknown, untrusted CA: CN=localhost, OU=GlassFish, O=Oracle Corporation, L=Santa Clara, ST=California, C=US -- [Path does not chain with any of the trust anchors].
172.16.1.25:8181	TLS/SSL certificate signed by unknown, untrusted CA: CN=creg.utp.edu.co, OU=GlassFish, O=Oracle Corporation, L=Santa Clara, ST=California, C=US -- [Path does not chain with any of the trust anchors].
172.16.1.46:5989	TLS/SSL certificate signed by unknown, untrusted CA: CN=PEGASUS TEST CERTIFICATE-DO NOT USE, OU=The OpenPegasus Project, O=The Open Group, L=Reading, ST=Berkshire, C=UK -- [Path does not chain with any of the trust anchors].
172.16.1.7:443	TLS/SSL certificate signed by unknown, untrusted CA: CN=Certificado Empresarial Clase-A, O=Certicamara S.A. Entidad de Certificacion, L=Carrera 9 16-21 Bogota, C=CO -- [Path does not chain with any of the trust anchors].
181.118.158.2:8443	TLS/SSL certificate signed by unknown, untrusted CA: EMAILADDRESS=support@fortinet.com, CN=fortinet-subca2001, OU=Certificate Authority, O=Fortinet, L=Sunnyvale, ST=California, C=US -- [Path does not chain with any of the trust anchors].

References:

--	--

Source	Reference
URL	http://httpd.apache.org/docs/2.2/mod/mod_ssl.html
URL	http://nginx.org/en/docs/http/configuring_https_servers.html
URL	https://support.microsoft.com/en-us/kb/954755

Vulnerability Solution:

Ensure the common name (CN) reflects the name of the entity presenting the certificate (e.g., the hostname). If the certificate(s) or any of the chain certificate(s) have expired or been revoked, obtain a new certificate from your Certificate Authority (CA) by following their documentation. If a self-signed certificate is being used, consider obtaining a signed certificate from a CA.

References: [Mozilla: Connection Untrusted ErrorSSLShopper: SSL Certificate Not Trusted ErrorWindows/IIS certificate chain config](#)
[Apache SSL config](#)[Nginx SSL config](#)[CertificateChain.io](#)

3.2.34. Apache HTTPD: HTTP Trailers processing bypass (CVE-2013-5704) (apache-httpd-cve-2013-5704)*Description:*

HTTP trailers could be used to replace HTTP headers late during request processing, potentially undoing or otherwise confusing modules that examined or modified request headers earlier. This fix adds the "MergeTrailers" directive to restore legacy behavior.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
APPLE	APPLE-SA-2015-04-08-2
APPLE	APPLE-SA-2015-09-16-4
BID	66550
CVE	CVE-2013-5704
REDHAT	RHSA-2015:0325
REDHAT	RHSA-2015:1249
REDHAT	RHSA-2015:2659
REDHAT	RHSA-2015:2660
REDHAT	RHSA-2015:2661
REDHAT	RHSA-2016:0061
REDHAT	RHSA-2016:0062
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Source	Reference
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.29

Upgrade to Apache HTTPD version 2.2.29

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.29.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.12

Upgrade to Apache HTTPD version 2.4.12

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.12.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.35. Apache HTTPD: mod_cache crash with empty Content-Type header (CVE-2014-3581) (apache-httpd-cve-2014-3581)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_cache. Review your web server configuration for validation. A NULL pointer deference was found in mod_cache. A malicious HTTP server could cause a crash in a caching forward proxy configuration. This crash would only be a denial of service if using a threaded MPM.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
APPLE	APPLE-SA-2015-08-13-2
APPLE	APPLE-SA-2015-09-16-4
BID	71656
CVE	CVE-2014-3581
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061337

Source	Reference
IAVM	2015-A-0199
REDHAT	RHSA-2015:0325
URL	http://httpd.apache.org/security/vulnerabilities_24.html
XF	97027

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.12

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.12.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.36. Apache HTTPD: mod_proxy_fcgi out-of-bounds memory read (CVE-2014-3583) (apache-httpd-cve-2014-3583)*Description:*

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy_fcgi. Review your web server configuration for validation. An out-of-bounds memory read was found in mod_proxy_fcgi. A malicious FastCGI server could send a carefully crafted response which could lead to a crash when reading past the end of a heap memory or stack buffer. This issue affects version 2.4.10 only.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
APPLE	APPLE-SA-2015-08-13-2
APPLE	APPLE-SA-2015-09-16-4
BID	71657
CVE	CVE-2014-3583
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061337
IAVM	2015-A-0199
REDHAT	RHSA-2015:1855
REDHAT	RHSA-2015:1858
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.12

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.12.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.37. Apache HTTPD: mod_lua: Crash in websockets PING handling (CVE-2015-0228) (apache-httpd-cve-2015-0228)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_lua. Review your web server configuration for validation. A stack recursion crash in the mod_lua module was found. A Lua script executing the r:wsupgrade() function could crash the process if a malicious client sent a carefully crafted PING request. This issue affected releases 2.4.7 through 2.4.12 inclusive.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
APPLE	APPLE-SA-2015-08-13-2
APPLE	APPLE-SA-2015-09-16-4
BID	73041
BID	91787
CVE	CVE-2015-0228
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061135
DISA_VMSKEY	V0061337
IAVM	2015-A-0174
IAVM	2015-A-0199
REDHAT	RHSA-2015:1666
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.16

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.16.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.38. Apache HTTPD: HTTP request smuggling attack against chunked request parser (CVE-2015-3183) (apache-httpd-cve-2015-3183)

Description:

An HTTP request smuggling attack was possible due to a bug in parsing of chunked requests. A malicious client could force the server to misinterpret the request length, allowing cache poisoning or credential hijacking if an intermediary proxy is in use.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
APPLE	APPLE-SA-2015-08-13-2
APPLE	APPLE-SA-2015-09-16-4
BID	75963
BID	91787
CVE	CVE-2015-3183
DEBIAN	DSA-3325
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061135
DISA_VMSKEY	V0061337
IAVM	2015-A-0174
IAVM	2015-A-0199
REDHAT	RHSA-2015:1666
REDHAT	RHSA-2015:1667
REDHAT	RHSA-2015:1668
REDHAT	RHSA-2015:2659
REDHAT	RHSA-2015:2660
REDHAT	RHSA-2015:2661
REDHAT	RHSA-2016:0061

Source	Reference
REDHAT	RHSA-2016:0062
REDHAT	RHSA-2016:2054
REDHAT	RHSA-2016:2055
REDHAT	RHSA-2016:2056
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

- Apache HTTPD >= 2.2 and < 2.2.31

Upgrade to Apache HTTPD version 2.2.31

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.31.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

- Apache HTTPD >= 2.4 and < 2.4.16

Upgrade to Apache HTTPD version 2.4.16

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.16.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.39. Apache HTTPD: Padding Oracle in Apache mod_session_crypto (CVE-2016-0736) (apache-httpd-cve-2016-0736)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_session_crypto. Review your web server configuration for validation. Prior to Apache HTTP release 2.4.25, mod_sessioncrypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC. An authentication tag (SipHash MAC) is now added to prevent such attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference

Source	Reference
BID	95078
CVE	CVE-2016-0736
DEBIAN	DSA-3796
DISA_SEVERITY	Category I
IAVM	2017-A-0010
REDHAT	RHSA-2017:0906
REDHAT	RHSA-2017:1161
REDHAT	RHSA-2017:1413
REDHAT	RHSA-2017:1414
REDHAT	RHSA-2017:1415
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.25

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.25.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.40. Apache HTTPD: DoS vulnerability in mod_auth_digest (CVE-2016-2161) (apache-httpd-cve-2016-2161)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_auth_digest. Review your web server configuration for validation. Malicious input to mod_auth_digest will cause the server to crash, and each instance continues to crash even for subsequently valid requests.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	95076
CVE	CVE-2016-2161
DEBIAN	DSA-3796
DISA_SEVERITY	Category I

Source	Reference
IAVM	2017-A-0010
REDHAT	RHSA-2017:0906
REDHAT	RHSA-2017:1161
REDHAT	RHSA-2017:1413
REDHAT	RHSA-2017:1414
REDHAT	RHSA-2017:1415
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.25

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.25.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.41. Apache HTTPD: HTTP_PROXY environment variable "httpoxy" mitigation (CVE-2016-5387) (apache-httpd-cve-2016-5387)

Description:

HTTP_PROXY is a well-defined environment variable in a CGI process, which collided with a number of libraries which failed to avoid colliding with this CGI namespace. A mitigation is provided for the httpd CGI environment to avoid populating the "HTTP_PROXY" variable from a "Proxy:" header, which has never been registered by IANA. This workaround and patch are documented in the ASF Advisory at asf-httpoxy-response.txt and incorporated in the 2.4.25 and 2.2.32 releases. Note: This is not assigned an httpd severity, as it is a defect in other software which overloaded well-established CGI environment variables, and does not reflect an error in HTTP server software.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	91816
CERT-VN	797896
CVE	CVE-2016-5387
DEBIAN	DSA-3623
DISA_SEVERITY	Category I

Source	Reference
IAVM	2016-B-0160
IAVM	2017-A-0010
REDHAT	RHSA-2016:1420
REDHAT	RHSA-2016:1421
REDHAT	RHSA-2016:1422
REDHAT	RHSA-2016:1624
REDHAT	RHSA-2016:1625
REDHAT	RHSA-2016:1635
REDHAT	RHSA-2016:1636
REDHAT	RHSA-2016:1648
REDHAT	RHSA-2016:1649
REDHAT	RHSA-2016:1650
REDHAT	RHSA-2016:1851
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.32

Upgrade to Apache HTTPD version 2.2.32

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.32.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.25

Upgrade to Apache HTTPD version 2.4.25

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.25.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.42. Apache HTTPD: Apache HTTP Request Parsing Whitespace Defects (CVE-2016-8743) (apache-httpd-cve-2016-8743)

Description:

Apache HTTP Server, prior to release 2.4.25 (2.2.32), accepted a broad pattern of unusual whitespace patterns from the user-agent, including bare CR, FF, VTAB in parsing the request line and request header lines, as well as HTAB in parsing the request line. Any bare CR present in request lines was treated as whitespace and remained in the request field member "the_request", while a bare CR

in the request header field name would be honored as whitespace, and a bare CR in the request header field value was retained the input headers array. Implied additional whitespace was accepted in the request line and prior to the ':' delimiter of any request header lines. RFC7230 Section 3.5 calls out some of these whitespace exceptions, and section 3.2.3 eliminated and clarified the role of implied whitespace in the grammar of this specification. Section 3.1.1 requires exactly one single SP between the method and request-target, and between the request-target and HTTP-version, followed immediately by a CRLF sequence. None of these fields permit any (unencoded) CTL character whatsoever. Section 3.2.4 explicitly disallowed any whitespace from the request header field prior to the ':' character, while Section 3.2 disallows all CTL characters in the request header line other than the HTAB character as whitespace. These defects represent a security concern when httpd is participating in any chain of proxies or interacting with back-end application servers, either through mod_proxy or using conventional CGI mechanisms. In each case where one agent accepts such CTL characters and does not treat them as whitespace, there is the possibility in a proxy chain of generating two responses from a server behind the uncautious proxy agent. In a sequence of two requests, this results in request A to the first proxy being interpreted as requests A + A' by the backend server, and if requests A and B were submitted to the first proxy in a keepalive connection, the proxy may interpret response A' as the response to request B, polluting the cache or potentially serving the A' content to a different downstream user-agent. These defects are addressed with the release of Apache HTTP Server 2.4.25 and coordinated by a new directive; HttpProtocolOptions Strict which is the default behavior of 2.4.25 and later. By toggling from 'Strict' behavior to 'Unsafe' behavior, some of the restrictions may be relaxed to allow some invalid HTTP/1.1 clients to communicate with the server, but this will reintroduce the possibility of the problems described in this assessment. Note that relaxing the behavior to 'Unsafe' will still not permit raw CTLs other than HTAB (where permitted), but will allow other RFC requirements to not be enforced, such as exactly two SP characters in the request line.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	95077
CVE	CVE-2016-8743
DEBIAN	DSA-3796
DISA_SEVERITY	Category I
IAVM	2017-A-0010
REDHAT	RHSA-2017:0906
REDHAT	RHSA-2017:1161
REDHAT	RHSA-2017:1413
REDHAT	RHSA-2017:1414
REDHAT	RHSA-2017:1415
REDHAT	RHSA-2017:1721
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Source	Reference
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.32

Upgrade to Apache HTTPD version 2.2.32

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.32.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.25

Upgrade to Apache HTTPD version 2.4.25

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.25.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.43. Apache HTTPD: Out of bound write in mod_authnz_ldap when using too small Accept-Language values (CVE-2017-15710) (apache-httpd-cve-2017-15710)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_authnz_ldap. Review your web server configuration for validation. mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	103512
CVE	CVE-2017-15710
DEBIAN	DSA-4164

Source	Reference
REDHAT	RHSA-2018:3558
REDHAT	RHSA-2019:0366
REDHAT	RHSA-2019:0367
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.33

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.33.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.44. Apache HTTPD: Use-after-free when using <Limit > with an unrecognized method in .htaccess ("OptionsBleed") (CVE-2017-9798) (apache-httpd-cve-2017-9798)

Description:

When an unrecognized HTTP Method is given in an <Limit {method}> directive in an .htaccess file, and that .htaccess file is processed by the corresponding request, the global methods table is corrupted in the current worker process, resulting in erratic behaviour. This behavior may be avoided by listing all unusual HTTP Methods in a global httpd.conf RegisterHttpMethod directive in httpd release 2.4.25 and later. To permit other .htaccess directives while denying the <Limit > directive, see the AllowOverrideList directive. Source code patch (2.4) is at; CVE-2017-9798-patch-2.4.patch Source code patch (2.2) is at; CVE-2017-9798-patch-2.2.patch Note 2.2 is end-of-life, no further release with this fix is planned. Users are encouraged to migrate to 2.4.28 or later for this and other fixes.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	100872
BID	105598
CVE	CVE-2017-9798
DEBIAN	DSA-3980
REDHAT	RHSA-2017:2882
REDHAT	RHSA-2017:2972
REDHAT	RHSA-2017:3018
REDHAT	RHSA-2017:3113

Source	Reference
REDHAT	RHSA-2017:3114
REDHAT	RHSA-2017:3193
REDHAT	RHSA-2017:3194
REDHAT	RHSA-2017:3195
REDHAT	RHSA-2017:3239
REDHAT	RHSA-2017:3240
REDHAT	RHSA-2017:3475
REDHAT	RHSA-2017:3476
REDHAT	RHSA-2017:3477
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.28

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.28.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.45. Apache HTTPD: Possible out of bound read in mod_cache_socache (CVE-2018-1303) (apache-httpd-cve-2018-1303)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_cache_socache. Review your web server configuration for validation. A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.33 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	103522
CVE	CVE-2018-1303

Source	Reference
DEBIAN	DSA-4164
REDHAT	RHSA-2018:3558
REDHAT	RHSA-2019:0366
REDHAT	RHSA-2019:0367
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.33

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.33.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.46. Apache HTTPD: mod_session_cookie does not respect expiry time (CVE-2018-17199) (apache-httpd-cve-2018-17199)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_session_cookie. Review your web server configuration for validation. In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	106742
CVE	CVE-2018-17199
DEBIAN	DSA-4422
REDHAT	RHSA-2019:3932
REDHAT	RHSA-2019:3933
REDHAT	RHSA-2019:3935
REDHAT	RHSA-2019:4126
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.38

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.38.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.47. Apache HTTPD: Apache httpd URL normalization inconsistency (CVE-2019-0220) (apache-httpd-cve-2019-0220)*Description:*

When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	107670
CVE	CVE-2019-0220
DEBIAN	DSA-4422
REDHAT	RHSA-2019:2343
REDHAT	RHSA-2019:3436
REDHAT	RHSA-2019:4126
REDHAT	RHSA-2020:0250
REDHAT	RHSA-2020:0251
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.39

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.39.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.48. Apache HTTPD: mod_proxy_ftp use of uninitialized value (CVE-2020-1934) (apache-httpd-cve-2020-1934)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy_ftp. Review your web server configuration for validation. Apache HTTP Server versions 2.4.0 to 2.4.41 mod_proxy_ftp use of uninitialized value with malicious FTP backend.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
CVE	CVE-2020-1934
DEBIAN	DSA-4757
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.42

Download and apply the upgrade from: <https://httpd.apache.org/download.cgi#apache24>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.49. Apache Tomcat default installation/welcome page installed (apache-tomcat-default-install-page)*Description:*

The Tomcat default installation or "Welcome" page is installed on this server. This usually indicates a newly installed server which has not yet been configured properly and which may not be known about.

In many cases, Tomcat is installed along with other applications and the user may not be aware that the web server is running. These servers are rarely patched and rarely monitored, providing hackers with a convenient target that is not likely to trip any alarms.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.7:8080	Running HTTP serviceProduct Tomcat exists -- Apache TomcatHTTP GET request to http://172.16.1.7:8080/ HTTP response code was an expected 200 190: <td style="width:20px"> </td> 191:

Affected Nodes:	Additional Information:
	192: <!-- Body --> 193: <td align="left" valign="top"> 194: ... means you've setup Tomcat successfully. Congratulations! </p>
172.16.1.7:8082	Running HTTP serviceProduct Tomcat exists -- Apache TomcatHTTP GET request to http://172.16.1.7:8082/ HTTP response code was an expected 200 190: <td style="width:20px"> </td> 191: 192: <!-- Body --> 193: <td align="left" valign="top"> 194: ... means you've setup Tomcat successfully. Congratulations! </p>

References:

Source	Reference
OSVDB	2117

Vulnerability Solution:

If this server is required to provide necessary functionality, then the default page should be replaced with relevant content. Otherwise, this server should be removed from the network, following the security principle of minimum complexity.

3.2.50. Database Open Access (database-open-access)*Description:*

The database allows any remote system the ability to connect to it. It is recommended to limit direct access to trusted systems because databases may contain sensitive data, and new vulnerabilities and exploits are discovered routinely for them. For this reason, it is a violation of PCI DSS section 1.3.6 to have databases listening on ports accessible from the Internet, even when protected with secure authentication mechanisms.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.111:3306	Running MySQL service
172.16.1.12:1521	Running Oracle TNS Listener service

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

Vulnerability Solution:

Configure the database server to only allow access to trusted systems. For example, the PCI DSS standard requires you to place the database in an internal network zone, segregated from the DMZ

3.2.51. Lotus Notes/Domino Anonymous Access to DECS Documentation ([http-domino-0028](#))

Description:

The Domino server has been configured to allow anonymous access to the DECS Documentation Database (/help/decsdoc.nsf). This is a documentation database that is installed by default with Domino. There is generally no good reason for an anonymous user to access this database from the web.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.46:80	Running HTTP serviceProduct Lotus Domino exists -- Lotus Domino 9.0.0.0 /help/decsdoc.nsf

References:

None

Vulnerability Solution:

Open the database in the Lotus Notes client and edit the ACL.

Change the access level for Default and Anonymous to "No Access".

If this information is not critical for distribution to other domains, also restrict access for OtherDomainServers to "No Access".

For all entries set to "No Access", also verify that the "Read public documents" and "Write public documents" are unchecked. If not, access will still be permitted for any public documents.

3.2.52. Lotus Notes/Domino Anonymous Access to Domino Connector Documentation ([http-domino-0033](#))

Description:

The Domino server has been configured to allow anonymous access to the Domino Connector Documentation Database (/help/lccon.nsf). This is a documentation database that is installed by default with Domino. There is generally no good reason for an anonymous user to access this database from the web.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.46:80	Running HTTP serviceProduct Lotus Domino exists -- Lotus Domino 9.0.0.0 /help/lccon.nsf

References:

None

Vulnerability Solution:

Open the database in the Lotus Notes client and edit the ACL.

Change the access level for Default and Anonymous to "No Access".

If this information is not critical for distribution to other domains, also restrict access for OtherDomainServers to "No Access".

For all entries set to "No Access", also verify that the "Read public documents" and "Write public documents" are unchecked. If not,

access will still be permitted for any public documents.

3.2.53. Lotus Notes/Domino Anonymous Access to LSX for Lotus Connectors Documentation (http-domino-0034)

Description:

The Domino server has been configured to allow anonymous access to the LSX for Lotus Connectors Database (/help/lxslc.nsf). This is a documentation database that is installed by default with Domino. There is generally no good reason for an anonymous user to access this database from the web.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.46:80	Running HTTP serviceProduct Lotus Domino exists -- Lotus Domino 9.0.0.0 /help/lxslc.nsf

References:

None

Vulnerability Solution:

Open the database in the Lotus Notes client and edit the ACL.

Change the access level for Default and Anonymous to "No Access".

If this information is not critical for distribution to other domains, also restrict access for OtherDomainServers to "No Access".

For all entries set to "No Access", also verify that the "Read public documents" and "Write public documents" are unchecked. If not, access will still be permitted for any public documents.

3.2.54. Microsoft IIS default installation/welcome page installed (http-iis-default-install-page)

Description:

The IIS default installation or "Welcome" page is installed on this server. This usually indicates a newly installed server which has not yet been configured properly and which may not be known about.

In many cases, IIS is installed by default and the user may not be aware that the web server is running. These servers are rarely patched and rarely monitored, providing hackers with a convenient target that is not likely to trip any alarms.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.156:80	Running HTTP serviceProduct IIS exists -- Microsoft IIS 8.5HTTP GET request to http://172.16.1.156/ HTTP response code was an expected 200 HTTP header 'Content-Location' not present HTTP response code was an expected 200HTTP response code was an expected 200HTTP response code was an expected 200HTTP response code was an expected 200HTTP response code was an expected 200HTTP response code was an expected 200

Affected Nodes:	Additional Information:
	200HTTP response code was an expected 200 1: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://ww... 2: <html xmlns="http://www.w3.org/1999/xhtml"> 3: <head> 4: <meta http-equiv="Content-Type" content="text/html; charset=iso-885... 5: <title>IIS Windows Server</title>

References:

Source	Reference
OSVDB	2117

Vulnerability Solution:

If this server is required to provide necessary functionality, then the default page should be replaced with relevant content. Otherwise, this server should be removed from the network, following the security principle of minimum complexity.

If the server is not needed, it can be disabled in the following way: in the Services window of the Control Panel's Administrative Tools section, right-click on the 'World Wide Web Server' entry and select 'Stop'. Set its startup type to 'Manual' so that it does not restart if the machine is rebooted (this is done by selecting 'Properties' in the right-click menu).

3.2.55. httpd: Log injection vulnerability in mod_auth (CVE-2015-3200) ([http-lighttpd-cve-2015-3200](#))*Description:*

mod_auth in lighttpd before 1.4.36 allows remote attackers to inject arbitrary log entries via a basic HTTP authentication string without a colon character, as demonstrated by a string containing a NULL and new line character.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.7:8008	Running HTTP serviceProduct lighttpd exists -- lighttpd 1.4.35Vulnerable version of product lighttpd found -- lighttpd 1.4.35

References:

Source	Reference
BID	74813
CVE	CVE-2015-3200
URL	https://redmine.lighttpd.net/issues/2646

Vulnerability Solution:

Download and apply the upgrade from: <http://www.lighttpd.net/download/>

3.2.56. httpd: potential path traversal with specific configs (CVE-2018-19052) ([http-lighttpd-cve-2018-19052](#))

Description:

An issue was discovered in `mod_alias_physical_handler` in `mod_alias.c` in `lighttpd` before 1.4.50. There is potential `../` path traversal of a single directory above an alias target, with a specific `mod_alias` configuration where the matched alias lacks a trailing `'/'` character, but the alias target filesystem path does have a trailing `'/'` character.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.7:8008	Running HTTP service Product <code>lighttpd</code> exists -- <code>lighttpd 1.4.35</code> Vulnerable version of product <code>lighttpd</code> found -- <code>lighttpd 1.4.35</code>

References:

Source	Reference
CVE	CVE-2018-19052
URL	https://download.lighttpd.net/lighttpd/security/lighttpd_cve-2018-19052.txt

Vulnerability Solution:

Download and apply the upgrade from: <http://www.lighttpd.net/download/>

3.2.57. memcached: Distributed Reflected Denial of Service via UDP (CVE-2018-1000115) (memcached-cve-2018-1000115)

Description:

Memcached connections using UDP can be abused for efficient traffic amplification distributed denial of service (DDoS) attacks. A remote attacker could send a malicious UDP request using a spoofed source IP address of a target system to memcached, causing it to send a significantly larger response to the target. Traffic amplification of 1:50,000 has been reported by reliable sources.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:11211	memcached service accessible over UDP

References:

Source	Reference
CERT	TA14-017A
CVE	CVE-2018-1000115
URL	https://blog.rapid7.com/2018/02/27/the-flip-side-of-memcrashed/

Vulnerability Solution:

Any of the following actions may be used to secure memcached installations and prevent them from being used in DDoS attacks.

- Configure a firewall to ensure that memcached can only be accessed from trusted hosts that require the service. Disallow any access to the service from the public Internet. The default port for memcached is 11211 (on both TCP and UDP).
- Disable UDP if it is not required. This can be done by starting memcached with the -U 0 option. Make this the default behaviour by editing the memcached configuration file (often located at /etc/sysconfig/memcached or /etc/memcached.conf) to have the line `OPTIONS="-U 0"`
- Restrict memcached to localhost if it does not need to be accessed from other servers. This can be done by specifying the option -l 127.0.0.1

Please see the [memcached server configuration guide](#) for further information.

3.2.58. NTP: Traffic amplification in clrtap feature of ntpd (ntp-r7-2014-12-unsettrap-drdos)

Description:

An NTP control (mode 6) message with the UNSETTRAP (31) opcode with an unknown association identifier will cause NTP to respond with two packets -- one error response packet indicating that the association identifier was invalid followed by another non-error, largely empty response. Because the number of packets sent as the response is greater than the single packet request, this can be used to conduct a DRDoS attack using vulnerable NTP servers as the unwitting third parties.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:123	Running NTP serviceOne 12-byte NTP version 2 mode 6 opcode 31 request with 0-byte payload resulted in a 2x packet amplification and no bandwidth amplification:12-byte NTP version 2 mode 6 opcode 31 response with 0-byte payload12-byte NTP version 2 mode 6 opcode 31 response with 0-byte payloadOne 12-byte NTP version 3 mode 6 opcode 31 request with 0-byte payload resulted in a 2x packet amplification and no bandwidth amplification:12-byte NTP version 3 mode 6 opcode 31 response with 0-byte payload12-byte NTP version 3 mode 6 opcode 31 response with 0-byte payload

References:

Source	Reference
URL	https://community.rapid7.com/community/metasploit/blog/2014/08/25/r7-2014-12-more-amplification-vulnerabilities-in-ntp-allow-even-more-drdos-attacks

Vulnerability Solution:

Apply a restrict option to all hosts that are not authorized to perform NTP queries. For example, to deny query requests from all clients, put the following in the NTP configuration file, typically /etc/ntp.conf, and restart the NTP service:

```
restrict default nomodify nopeer noquery notrap
```

3.2.59. PHP Vulnerability: CVE-2017-16642 (php-cve-2017-16642)*Description:*

In PHP before 5.6.32, 7.x before 7.0.25, and 7.1.x before 7.1.11, an error in the date extension's timelib_meridian handling of 'front of' and 'back of' directives could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: this is a different issue than CVE-2017-11145.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
BID	101745
CVE	CVE-2017-16642
DEBIAN	DSA-4080
DEBIAN	DSA-4081
REDHAT	RHSA-2018:1296
REDHAT	RHSA-2019:2519
URL	https://bugs.php.net/bug.php?id=75055

Vulnerability Solution:

- Upgrade to PHP version 5.6.32
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.0.25
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.1.11
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.60. PHP Vulnerability: CVE-2018-10546 (php-cve-2018-10546)*Description:*

An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. An infinite loop exists in ext/iconv/iconv.c because the iconv stream filter does not reject invalid multibyte sequences.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
BID	104019
CVE	CVE-2018-10546
DEBIAN	DSA-4240
REDHAT	RHSA-2019:2519
URL	https://bugs.php.net/bug.php?id=76249

Vulnerability Solution:

- Upgrade to PHP version 5.6.36
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.0.30
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.1.17
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.5
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.61. PHP Vulnerability: CVE-2018-10548 (php-cve-2018-10548)*Description:*

An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. ext/ldap/ldap.c allows remote LDAP servers to cause a denial of service (NULL pointer dereference and application crash) because of mishandling of the ldap_get_dn return value.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
BID	104019

Source	Reference
CVE	CVE-2018-10548
DEBIAN	DSA-4240
REDHAT	RHSA-2019:2519
URL	https://bugs.php.net/bug.php?id=76248

Vulnerability Solution:

- Upgrade to PHP version 5.6.36
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.0.30
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.1.17
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.5
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.62. PHP Vulnerability: CVE-2018-14883 (php-cve-2018-14883)*Description:*

An issue was discovered in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. An Integer Overflow leads to a heap-based buffer over-read in `exif_thumbnail_extract` of `exif.c`.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
BID	104871
CVE	CVE-2018-14883
DEBIAN	DSA-4353
URL	https://bugs.php.net/bug.php?id=76423

Vulnerability Solution:

- Upgrade to PHP version 5.6.37
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.0.31
Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.1.20

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.2.8

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.63. PHP Vulnerability: CVE-2018-14884 (php-cve-2018-14884)

Description:

An issue was discovered in PHP 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1. Inappropriately parsing an HTTP response leads to a segmentation fault because `http_header_value` in `ext/standard/http_fopen_wrapper.c` can be a NULL value that is mishandled in an `atoi` call.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2018-14884
REDHAT	RHSA-2019:2519
URL	https://bugs.php.net/bug.php?id=75535

Vulnerability Solution:

- Upgrade to PHP version 7.0.27

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.1.13

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.2.1

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.64. PHP Vulnerability: CVE-2018-19396 (php-cve-2018-19396)

Description:

`ext/standard/var_unserializer.c` in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an `unserialize` call for the `com`, `dotnet`, or `variant` class.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
BID	105989
CVE	CVE-2018-19396
URL	https://bugs.php.net/bug.php?id=77177

Vulnerability Solution:

- Upgrade to PHP version 5.6.37
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.1.25
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.65. PHP Vulnerability: CVE-2018-19935 (php-cve-2018-19935)*Description:*

ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
BID	106143
CVE	CVE-2018-19935
DEBIAN	DSA-4353
URL	https://bugs.php.net/bug.php?id=77020

Vulnerability Solution:

- Upgrade to PHP version 5.6.39
Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.0.33

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.1.25

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.2.14

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.66. PHP Vulnerability: CVE-2018-20783 (php-cve-2018-20783)

Description:

In PHP before 5.6.39, 7.x before 7.0.33, 7.1.x before 7.1.25, and 7.2.x before 7.2.13, a buffer over-read in PHAR reading functions may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse a .phar file. This is related to phar_parse_pharfile in ext/phar/phar.c.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2018-20783
REDHAT	RHSA-2019:2519
REDHAT	RHSA-2019:3299
URL	https://bugs.php.net/bug.php?id=77143

Vulnerability Solution:

- Upgrade to PHP version 5.6.39

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.1.25

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.2.13

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.67. PHP Vulnerability: CVE-2019-11038 (php-cve-2019-11038)

Description:

When using the gdImageCreateFromXbm() function in the GD Graphics Library (aka LibGD) 2.2.5, as used in the PHP GD extension in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6, it is possible to supply data that will cause the function to

use the value of uninitialized variable. This may lead to disclosing contents of the stack that has been left there by previous code.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2019-11038
DEBIAN	DSA-4529
REDHAT	RHSA-2019:2519
REDHAT	RHSA-2019:3299
URL	https://bugs.php.net/bug.php?id=77973

Vulnerability Solution:

- Upgrade to PHP version 7.1.30
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.19
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.3.6
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.68. PHP Vulnerability: CVE-2019-9637 (php-cve-2019-9637)

Description:

An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference

Source	Reference
CVE	CVE-2019-9637
DEBIAN	DSA-4403
REDHAT	RHSA-2019:2519
REDHAT	RHSA-2019:3299
URL	https://bugs.php.net/bug.php?id=77630

Vulnerability Solution:

- Upgrade to PHP version 7.1.27
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.16
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.3.3
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.69. PHP Vulnerability: CVE-2019-9638 (php-cve-2019-9638)*Description:*

An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in `exif_process_IFD_in_MAKERNOTE` because of mishandling the `maker_note->offset` relationship to `value_len`.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2019-9638
DEBIAN	DSA-4403
REDHAT	RHSA-2019:2519
REDHAT	RHSA-2019:3299
URL	https://bugs.php.net/bug.php?id=77563

Vulnerability Solution:

- Upgrade to PHP version 7.1.27
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.16
Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.3.3

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.70. PHP Vulnerability: CVE-2019-9639 (php-cve-2019-9639)

Description:

An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in `exif_process_IFD_in_MAKERNOTE` because of mishandling the `data_len` variable.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2019-9639
DEBIAN	DSA-4403
REDHAT	RHSA-2019:2519
REDHAT	RHSA-2019:3299
URL	https://bugs.php.net/bug.php?id=77659

Vulnerability Solution:

- Upgrade to PHP version 7.1.27

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.2.16

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.3.3

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.71. PHP Vulnerability: CVE-2019-9640 (php-cve-2019-9640)

Description:

An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an Invalid Read in `exif_process_SOFn`.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2019-9640
DEBIAN	DSA-4403
REDHAT	RHSA-2019:2519
REDHAT	RHSA-2019:3299
URL	https://bugs.php.net/bug.php?id=77540

Vulnerability Solution:

- Upgrade to PHP version 7.1.27
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.16
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.3.3
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.72. PHP Vulnerability: CVE-2020-11579 (php-cve-2020-11579)*Description:*

An issue was discovered in Chadha PHPKB 9.0 Enterprise Edition. installer/test-connection.php (part of the installation process) allows a remote unauthenticated attacker to disclose local files on hosts running PHP before 7.2.16, or on hosts where the MySQL ALLOW LOCAL DATA INFILE option is enabled.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2020-11579

Vulnerability Solution:

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.73. SSH Birthday attacks on 64-bit block ciphers (SWEET32) (ssh-cve-2016-2183-sweet32)

Description:

Legacy block ciphers having a block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. The security of a block cipher is often reduced to the key size k : the best attack should be the exhaustive search of the key, with complexity 2^k to the power of k . However, the block size n is also an important security parameter, defining the amount of data that can be encrypted under the same key. This is particularly important when using common modes of operation: we require block ciphers to be secure with up to $2^{n/2}$ to the power of n queries, but most modes of operation (e.g. CBC, CTR, GCM, OCB, etc.) are unsafe with more than $2^{n/4}$ to the power of half n blocks of message (the birthday bound). With a modern block cipher with 128-bit blocks such as AES, the birthday bound corresponds to 256 exabytes. However, for a block cipher with 64-bit blocks, the birthday bound corresponds to only 32 GB, which is easily reached in practice. Once a collision between two cipher blocks occurs it is possible to use the collision to extract the plain text data.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:22	Running SSH serviceInsecure 3DES ciphers in use: 3des-cbc
172.16.1.103:22	Running SSH serviceInsecure 3DES ciphers in use: 3des-cbc
172.16.1.111:22	Running SSH serviceInsecure 3DES ciphers in use: 3des-cbc
172.16.1.12:22	Running SSH serviceInsecure 3DES ciphers in use: 3des-cbc
172.16.1.46:22	Running SSH serviceInsecure 3DES ciphers in use: 3des-cbc
172.16.1.7:22	Running SSH serviceInsecure 3DES ciphers in use: 3des-cbc

References:

Source	Reference
CVE	CVE-2016-2183
URL	https://sweet32.info/

Vulnerability Solution:

Remove all 3DES ciphers from the cipher list specified in `sshd_config`.

3.2.74. TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32) (ssl-cve-2016-2183-sweet32)

Description:

Legacy block ciphers having a block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of the SSL/TLS protocols that support cipher suites which use 3DES as the symmetric encryption cipher are affected. The security of a block cipher is often reduced to the key size k : the best attack should be the exhaustive search of the key, with complexity 2^k to the power of k . However, the block size n is also an important security parameter, defining the amount of data that can be encrypted under the same key. This is particularly important when using common modes of operation: we require block ciphers to be secure with up to $2^{n/2}$ to the power of n queries, but most modes of operation (e.g. CBC, CTR, GCM, OCB, etc.) are unsafe with more than $2^{n/4}$ to the power of half n blocks of message (the birthday bound). With a modern block cipher with 128-bit blocks such as AES, the birthday bound

corresponds to 256 exabytes. However, for a block cipher with 64-bit blocks, the birthday bound corresponds to only 32 GB, which is easily reached in practice. Once a collision between two cipher blocks occurs it is possible to use the collision to extract the plain text data.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.1 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.2 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
172.16.1.12:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
172.16.1.156:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA
172.16.1.156:3389	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA
172.16.1.180:8181	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.1 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.2 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
172.16.1.25:8181	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
172.16.1.46:5989	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers:

Affected Nodes:	Additional Information:
	TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA
172.16.1.7:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.0 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA

References:

Source	Reference
CVE	CVE-2016-2183
URL	https://sweet32.info/
URL	https://www.openssl.org/blog/blog/2016/08/24/sweet32
URL	https://access.redhat.com/articles/2548661

Vulnerability Solution:

Configure the server to disable support for 3DES suite.

For Microsoft IIS web servers, see Microsoft Knowledgebase article [245030](#) for instructions on disabling 3DES cipher suite.

The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.

Refer to your server vendor documentation to apply the recommended cipher configuration:

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

3.2.75. MD5-based Signature in TLS/SSL Server X.509 Certificate (tls-server-cert-sig-md5)*Description:*

Multiple weaknesses exist in the MD5 cryptographic hash function, which make it insecure when used to sign X.509 certificates. Namely:

- In August 2004, Xiaoyun Wang, Dengguo Feng, Xuejia Lai, and Hongbo Yu published the results of a [collision attack](#).
- In October 2006, Marc Stevens, Arjen K. Lenstra, and Benne de Weger produced a [pair of colliding X.509 certificates for different identities](#). The method used to produce them was later published in the EuroCrypt 2007 Proceedings, and described as one practical application of [chosen-prefix collision attacks](#).
- In December 2008, a larger team of security researchers used this attack to create a [rogue CA certificate](#), allowing them to impersonate any website on the Internet, including banking and e-commerce sites secured using the HTTPS protocol.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:443	SSL certificate is signed with MD5withRSA
172.16.1.46:5989	SSL certificate is signed with MD5withRSA

References:

Source	Reference
BID	33065
CERT-VN	836068
CVE	CVE-2004-2761
REDHAT	RHSA-2010:0837
REDHAT	RHSA-2010:0838
URL	http://blogs.technet.com/swi/archive/2008/12/30/information-regarding-md5-collisions-problem.aspx
URL	http://www.microsoft.com/technet/security/advisory/961509.msp

Vulnerability Solution:

Stop using signature algorithms relying on MD5, such as "MD5withRSA", when signing X.509 certificates. Instead, use the SHA-2 family (SHA-224, SHA-256, SHA-384, and SHA-512).

3.2.76. Apache HTTPD: ETag Inode Information Leakage (CVE-2003-1418) (apache-httpd-cve-2003-1418)*Description:*

Apache HTTP server in certain configurations allows remote attackers to obtain sensitive information via (1) the ETag header, which reveals the inode number, or (2) multipart MIME boundary, which reveals child process IDs (PID).

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.7:80	The Apache server returned a vulnerable ETag header
172.16.1.7:443	The Apache server returned a vulnerable ETag header
172.16.1.7:7778	The Apache server returned a vulnerable ETag header

References:

Source	Reference
BID	6939
BID	6943

Source	Reference
CVE	CVE-2003-1418
XF	11438

Vulnerability Solution:

- Disable inode-based ETag generation in the Apache config

You can remove inode information from the ETag header by adding the following directive to your Apache config:

```
FileETag MTime Size
```

- OpenBSD

Apply OpenBSD 3.2 errata #8 for Apache inode and pid leak

Download and apply the patch from: <http://www.openbsd.org/errata32.html#httpd>

The OpenBSD team has released a [patch](#) for the Apache inode and pid leak problem. This patch can be applied cleanly to 3.2 stable and rebuilt. Restart httpd for the changes to take effect. OpenBSD 3.3 will ship with the patched httpd by default. The patch can be applied to earlier 3.x versions of OpenBSD, but it may require editing of the source code.

3.2.77. Apache HTTPD: Method 413 Error Response Cross-Site Scripting Vulnerability (CVE-2007-6203) (apache-httpd-cve-2007-6203)

Description:

Apache HTTP Server 2.0.x and 2.2.x does not sanitize the HTTP Method specifier header from an HTTP request when it is reflected back in a "413 Request Entity Too Large" error message, which might allow cross-site scripting (XSS) style attacks using web client components that can send arbitrary headers in requests, as demonstrated via an HTTP request containing an invalid Content-length value, a similar issue to CVE-2006-3918.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.7:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPDHTTP <SCRIPT>NXSSTEST</SCRIPT> request to http://172.16.1.7/ 3: <title>413 Request Entity Too Large</title> 4: </head><body> 5: <h1>Request Entity Too Large</h1> 6: The requested resource /index.html 7: does not allow request data with <SCRIPT>NXSSTEST</SCRIPT> requests
172.16.1.7:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDHTTP <SCRIPT>NXSSTEST</SCRIPT> request to https://172.16.1.7/ 3: <title>413 Request Entity Too Large</title> 4: </head><body> 5: <h1>Request Entity Too Large</h1> 6: The requested resource /index.html

Affected Nodes:	Additional Information:
	7: does not allow request data with <SCRIPT>NXSSTEST</SCRIPT> requests
172.16.1.7:7778	Running HTTP serviceProduct HTTPD exists -- Apache HTTPDHTTP <SCRIPT>NXSSTEST</SCRIPT> request to http://172.16.1.7:7778/ 3: <title>413 Request Entity Too Large</title> 4: </head><body> 5: <h1>Request Entity Too Large</h1> 6: The requested resource /index.html 7: does not allow request data with <SCRIPT>NXSSTEST</SCRIPT> requests

References:

Source	Reference
APPLE	APPLE-SA-2008-03-18
BID	26663
CVE	CVE-2007-6203
OVAL	12166
SUSE	SUSE-SA:2008:021
XF	38800

Vulnerability Solution:

- Apache HTTPD >= 2.0 and < 2.0.60

Upgrade to Apache HTTPD version 2.0.60

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.0.60.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

- Apache HTTPD >= 2.2 and < 2.2.5

Upgrade to Apache HTTPD version 2.2.5

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.5.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.78. Apache HTTPD: mod_lua multiple "Require" directive handling is broken (CVE-2014-8109) (apache-httpd-cve-2014-8109)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_lua. Review your web server configuration for validation. Fix handling of the Require line in mod_lau when a LuaAuthzProvider is used in multiple Require

directives with different arguments. This could lead to different authentication rules than expected.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
APPLE	APPLE-SA-2015-08-13-2
APPLE	APPLE-SA-2015-09-16-4
BID	73040
CVE	CVE-2014-8109
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061337
IAVM	2015-A-0199
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.12

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.12.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.79. Apache HTTPD: ap_some_auth_required API unusable (CVE-2015-3185) (apache-httpd-cve-2015-3185)

Description:

A design error in the "ap_some_auth_required" function renders the API unusable in httpd 2.4.x. In particular the API is documented to answering if the request required authentication but only answers if there are Require lines in the applicable configuration. Since 2.4.x Require lines are used for authorization as well and can appear in configurations even when no authentication is required and the request is entirely unrestricted. This could lead to modules using this API to allow access when they should otherwise not do so. API users should use the new ap_some_authn_required API added in 2.4.16 instead.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
APPLE	APPLE-SA-2015-08-13-2
APPLE	APPLE-SA-2015-09-16-2
APPLE	APPLE-SA-2015-09-16-4
BID	75965
CVE	CVE-2015-3185
DEBIAN	DSA-3325
DISA_SEVERITY	Category I
DISA_VMSKEY	V0061135
DISA_VMSKEY	V0061337
IAVM	2015-A-0174
IAVM	2015-A-0199
REDHAT	RHSA-2015:1666
REDHAT	RHSA-2015:1667
REDHAT	RHSA-2016:2957
REDHAT	RHSA-2017:2708
REDHAT	RHSA-2017:2709
REDHAT	RHSA-2017:2710
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.16

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.16.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.80. Apache HTTPD: mod_userdir CRLF injection (CVE-2016-4975) (apache-httpd-cve-2016-4975)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_userdir. Review your web server configuration for validation. Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	105093
CVE	CVE-2016-4975
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

- Apache HTTPD >= 2.2 and < 2.2.32

Upgrade to Apache HTTPD version 2.2.32

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.2.32.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

- Apache HTTPD >= 2.4 and < 2.4.25

Upgrade to Apache HTTPD version 2.4.25

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.25.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.81. Apache HTTPD: Tampering of mod_session data for CGI applications (CVE-2018-1283) (apache-httpd-cve-2018-1283)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_session. Review your web server configuration for validation. When mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications. The severity is set to Moderate because "SessionEnv on" is not a default nor common configuration, it should be considered more severe when this is the case though, because of the possible remote exploitation.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	103520
CVE	CVE-2018-1283
DEBIAN	DSA-4164
REDHAT	RHSA-2018:3558
REDHAT	RHSA-2019:0366
REDHAT	RHSA-2019:0367
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.33

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.33.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.82. Apache HTTPD: Possible out of bound access after failure in reading the HTTP request (CVE-2018-1301) (apache-httpd-cve-2018-1301)

Description:

A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.33, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
BID	103515
CVE	CVE-2018-1301

Source	Reference
DEBIAN	DSA-4164
REDHAT	RHSA-2018:3558
REDHAT	RHSA-2019:0366
REDHAT	RHSA-2019:0367
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.33

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.33.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.83. Apache HTTPD: Limited cross-site scripting in mod_proxy error page (CVE-2019-10092) (apache-httpd-cve-2019-10092)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy. Review your web server configuration for validation. A limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed. We have taken this opportunity to also remove request data from many other in-built error messages. Note however this issue did not affect them directly and their output was already escaped to prevent cross-site scripting attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
CVE	CVE-2019-10092
DEBIAN	DSA-4509
REDHAT	RHSA-2019:4126
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.41

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.41.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.84. Apache HTTPD: IP address spoofing when proxying using mod_remoteip and mod_rewrite (CVE-2020-11985) (apache-httpd-cve-2020-11985)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_remoteip, mod_rewrite. Review your web server configuration for validation. For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.180:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.10 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.10

References:

Source	Reference
CVE	CVE-2020-11985
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.25

Download and apply the upgrade from: <http://archive.apache.org/dist/httpd/httpd-2.4.25.tar.gz>

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.85. Drupal: CVE-2019-11358: Drupal core - Moderately critical - Cross Site Scripting - SA-CORE-2019-006 (drupal-cve-2019-11358)

Description:

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

Affected Nodes:

Affected Nodes:	Additional Information:
-----------------	-------------------------

Affected Nodes:	Additional Information:
172.16.1.1	Vulnerable software installed: Drupal 7.60

References:

Source	Reference
BID	108023
CVE	CVE-2019-11358
DEBIAN	DSA-4434
DEBIAN	DSA-4460
REDHAT	RHBA-2019:1570
REDHAT	RHSA-2019:1456
REDHAT	RHSA-2019:2587
REDHAT	RHSA-2019:3023
REDHAT	RHSA-2019:3024
URL	https://www.drupal.org/sa-core-2019-006

Vulnerability Solution:

- Upgrade to drupal version 7.66
Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>
- Upgrade to drupal version 8.5.1
Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>
- Upgrade to drupal version 8.6.1
Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

3.2.86. Drupal: CVE-2019-6341: Drupal core - Moderately critical - Cross Site Scripting - SA-CORE-2019-004 (drupal-cve-2019-6341)

Description:

In Drupal 7 versions prior to 7.65; Drupal 8.6 versions prior to 8.6.13; Drupal 8.5 versions prior to 8.5.14. Under certain circumstances the File module/subsystem allows a malicious user to upload a file that can trigger a cross-site scripting (XSS) vulnerability.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1	Vulnerable software installed: Drupal 7.60

References:

Source	Reference

Source	Reference
CVE	CVE-2019-6341
URL	https://www.drupal.org/sa-core-2019-004

Vulnerability Solution:

- Upgrade to drupal version 7.65

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

- Upgrade to drupal version 8.5.1

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

- Upgrade to drupal version 8.6.1

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

3.2.87. Drupal: CVE-2020-11022: Drupal core - Moderately critical - Cross Site Scripting - SA-CORE-2020-002 (drupal-cve-2020-11022)

Description:

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1	Vulnerable software installed: Drupal 7.60

References:

Source	Reference
CVE	CVE-2020-11022
DEBIAN	DSA-4693
URL	https://www.drupal.org/sa-core-2020-002

Vulnerability Solution:

- Upgrade to drupal version 7.70

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

- Upgrade to drupal version 8.7.1

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

- Upgrade to drupal version 8.8.6

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

3.2.88. Drupal: CVE-2020-11023: Drupal core - Moderately critical - Cross Site Scripting - SA-CORE-2020-002 (drupal-cve-2020-11023)

Description:

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1	Vulnerable software installed: Drupal 7.60

References:

Source	Reference
CVE	CVE-2020-11023
DEBIAN	DSA-4693
URL	https://www.drupal.org/sa-core-2020-002

Vulnerability Solution:

- Upgrade to drupal version 7.70
Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>
- Upgrade to drupal version 8.7.1
Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>
- Upgrade to drupal version 8.8.6
Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

3.2.89. Drupal: CVE-2020-13663: Drupal core - Critical - Cross Site Request Forgery - SA-CORE-2020-004 (drupal-cve-2020-13663)

Description:

The Drupal core Form API does not properly handle certain form input from cross-site requests, which can lead to other vulnerabilities.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1	Vulnerable software installed: Drupal 7.60

References:

Source	Reference
CVE	CVE-2020-13663

Source	Reference
URL	https://www.drupal.org/sa-core-2020-004

Vulnerability Solution:

- Upgrade to drupal version 7.72

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

- Upgrade to drupal version 8.8.8

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

- Upgrade to drupal version 8.9.1

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

- Upgrade to drupal version 9.0.1

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

3.2.90. Drupal: CVE-2020-13666: Drupal core - Moderately critical - Cross-site scripting - SA-CORE-2020-007 (drupal-cve-2020-13666)

Description:

The Drupal AJAX API does not disable JSONP by default, which can lead to cross-site scripting.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1	Vulnerable software installed: Drupal 7.60

References:

Source	Reference
CVE	CVE-2020-13666
URL	https://www.drupal.org/sa-core-2020-007

Vulnerability Solution:

- Upgrade to drupal version 7.73

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

- Upgrade to drupal version 8.8.1

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

- Upgrade to drupal version 8.9.6

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

- Upgrade to drupal version 9.0.6

Download and apply the upgrade from: <https://www.drupal.org/project/drupal/releases>

3.2.91. PHP Vulnerability: CVE-2018-10547 (php-cve-2018-10547)

Description:

An issue was discovered in ext/phar/phar_object.c in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. There is Reflected XSS on the PHAR 403 and 404 error pages via request data of a request for a .phar file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2018-5712.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2018-10547
DEBIAN	DSA-4240
REDHAT	RHSA-2019:2519
URL	https://bugs.php.net/bug.php?id=76129

Vulnerability Solution:

- Upgrade to PHP version 5.6.36
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.0.30
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.1.17
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.5
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.92. PHP Vulnerability: CVE-2018-14851 (php-cve-2018-14851)*Description:*

exif_process_IFD_in_MAKERNOTE in ext/exif/exif.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG file.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
BID	104871
CVE	CVE-2018-14851
DEBIAN	DSA-4353
REDHAT	RHSA-2019:2519
URL	https://bugs.php.net/bug.php?id=76557

Vulnerability Solution:

- Upgrade to PHP version 5.6.37
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.0.31
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.1.20
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.8
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.93. PHP Vulnerability: CVE-2018-17082 (php-cve-2018-17082)*Description:*

The Apache2 component in PHP before 5.6.38, 7.0.x before 7.0.32, 7.1.x before 7.1.22, and 7.2.x before 7.2.10 allows XSS via the body of a "Transfer-Encoding: chunked" request, because the bucket brigade is mishandled in the php_handler function in sapi/apache2handler/sapi_apache2.c.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2018-17082
DEBIAN	DSA-4353
REDHAT	RHSA-2019:2519
URL	https://bugs.php.net/bug.php?id=76582

Vulnerability Solution:

- Upgrade to PHP version 5.6.38

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.0.32

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.1.22

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.2.10

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.94. PHP Vulnerability: CVE-2018-5711 (php-cve-2018-5711)*Description:*

gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1, has an integer signedness error that leads to an infinite loop via a crafted GIF file, as demonstrated by a call to the imagecreatefromgif or imagecreatefromstring PHP function. This is related to GetCode_ and gdImageCreateFromGifCtx.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
CVE	CVE-2018-5711
REDHAT	RHSA-2018:1296
REDHAT	RHSA-2019:2519
URL	https://bugs.php.net/bug.php?id=75571

Vulnerability Solution:

- Upgrade to PHP version 5.6.33

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.0.27

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.1.13

Download and apply the upgrade from: <http://www.php.net/releases/>

- Upgrade to PHP version 7.2.1

Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.95. PHP Vulnerability: CVE-2018-5712 (php-cve-2018-5712)

Description:

An issue was discovered in PHP before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1. There is Reflected XSS on the PHAR 404 error page via the URI of a request for a .phar file.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
BID	102742
BID	104020
CVE	CVE-2018-5712
REDHAT	RHSA-2018:1296
REDHAT	RHSA-2019:2519
URL	https://bugs.php.net/bug.php?id=74782

Vulnerability Solution:

- Upgrade to PHP version 5.6.33
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.0.27
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.1.13
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.1
Download and apply the upgrade from: <http://www.php.net/releases/>

3.2.96. TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566) (rc4-cve-2013-2566)

Description:

Recent cryptanalysis results exploit biases in the RC4 keystream to recover repeatedly encrypted plaintexts. As a result, RC4 can no longer be seen as providing a sufficient level of security for SSL/TLS sessions. It has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_EXPORT_WITH_RC4_40_MD5TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA
172.16.1.156:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHATLS 1.0 ciphers: TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA TLS 1.1 ciphers: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHATLS 1.2 ciphers: TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA
172.16.1.156:3389	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHATLS 1.1 ciphers: TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA TLS 1.2 ciphers: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA
172.16.1.25:8181	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_ECDHE_RSA_WITH_RC4_128_SHATLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA
172.16.1.46:5989	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHATLS 1.0 ciphers: TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA
172.16.1.7:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_EXPORT_WITH_RC4_40_MD5TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHATLS 1.0 ciphers: TLS_RSA_EXPORT_WITH_RC4_40_MD5TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA

References:

Source	Reference
CVE	CVE-2013-2566
URL	http://www.isg.rhul.ac.uk/tls/
URL	https://tools.ietf.org/html/rfc7465
URL	http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295
URL	https://wiki.mozilla.org/Security/Server_Side_TLS
URL	https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Rule_-_Only_Support_Strong_Cryptographic_Ciphers
URL	http://support.microsoft.com/kb/245030/

Vulnerability Solution:

Configure the server to disable support for RC4 ciphers.

For Microsoft IIS web servers, see Microsoft Knowledgebase article [245030](#) for instructions on disabling rc4 ciphers.

The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.

Refer to your server vendor documentation to apply the recommended cipher configuration:

```
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK
```

3.2.97. SSH Server Supports diffie-hellman-group1-sha1 (ssh-cve-2015-4000)

Description:

The prime modulus offered when diffie-hellman-group1-sha1 is used only has a size of 1024 bits. This size is considered weak and within theoretical range of the so-called Logjam attack.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:22	Running SSH serviceInsecure key exchange in use: diffie-hellman-group1-sha1
172.16.1.103:22	Running SSH serviceInsecure key exchange in use: diffie-hellman-group1-sha1
172.16.1.111:22	Running SSH serviceInsecure key exchange in use: diffie-hellman-group1-sha1
172.16.1.12:22	Running SSH serviceInsecure key exchange in use: diffie-hellman-group1-sha1
172.16.1.180:22	Running SSH serviceInsecure key exchange in use: diffie-hellman-group1-sha1
172.16.1.46:22	Running SSH serviceInsecure key exchange in use: diffie-hellman-group1-sha1
172.16.1.7:22	Running SSH serviceInsecure key exchange in use: diffie-hellman-group1-sha1

References:

Source	Reference
CVE	CVE-2015-4000
URL	https://weakdh.org/

Vulnerability Solution:

Remove ssh-diffie-hellman-group1-sha1 from the KexAlgorithms list specified in sshd_config.

3.2.98. SSH Server Supports RC4 Cipher Algorithms (ssh-rc4-ciphers)

Description:

Cryptanalysis results exploit biases in the RC4 keystream to recover repeatedly encrypted plaintexts. As a result, RC4 can no longer be seen as providing a sufficient level of security for SSH sessions. It has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:22	Running SSH serviceInsecure arcfour (RC4) ciphers in use: arcfour256,arcfour128,arcfour
172.16.1.46:22	Running SSH serviceInsecure arcfour (RC4) ciphers in use: arcfour256,arcfour128,arcfour
172.16.1.7:22	Running SSH serviceInsecure arcfour (RC4) ciphers in use: arcfour256,arcfour128,arcfour

References:

Source	Reference
URL	http://www.openssh.com/txt/release-6.7

Vulnerability Solution:

Remove arcfour, arcfour128, and arcfour256 from the Ciphers list specified in sshd_config.

3.2.99. SSH Server Supports Weak Key Exchange Algorithms (ssh-weak-kex-algorithms)

Description:

The server supports one or more weak key exchange algorithms. It is highly advisable to remove weak key exchange algorithm support from SSH configuration files on hosts to prevent them from being used to establish connections.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:22	Running SSH serviceInsecure key exchange algorithms in use: diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
172.16.1.103:22	Running SSH serviceInsecure key exchange algorithms in use: diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
172.16.1.111:22	Running SSH serviceInsecure key exchange algorithms in use: diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
172.16.1.12:22	Running SSH serviceInsecure key exchange algorithms in use: diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
172.16.1.180:22	Running SSH serviceInsecure key exchange algorithms in use: diffie-hellman-

Affected Nodes:	Additional Information:
	group1-sha1
172.16.1.46:22	Running SSH serviceInsecure key exchange algorithms in use: diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
172.16.1.7:22	Running SSH serviceInsecure key exchange algorithms in use: diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1

References:

Source	Reference
URL	https://wiki.mozilla.org/Security/Guidelines/OpenSSH

Vulnerability Solution:

Refer to [this guide](#) on what KEX algorithms to permit in your SSH configuration.

3.2.100. SSH Weak Message Authentication Code Algorithms (ssh-weak-message-authentication-code-algorithms)*Description:*

The SSH server supports cryptographically weak Hash-based message authentication codes (HMACs) including MD5 or 96-bit Hash-based algorithms.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:22	Running SSH serviceInsecure MAC algorithms in use: hmac-md5,hmac-sha1-96,hmac-md5-96
172.16.1.46:22	Running SSH serviceInsecure MAC algorithms in use: hmac-md5,hmac-sha1-96,hmac-md5-96
172.16.1.7:22	Running SSH serviceInsecure MAC algorithms in use: hmac-md5,hmac-sha1-96,hmac-md5-96

References:

Source	Reference
URL	http://csrc.nist.gov/archive/ipsec/papers/rfc2403-hmacmd5.txt

Vulnerability Solution:

Consult the product documentation for instructions to disable any insecure MD5 or 96-bit HMAC algorithms within the SSH configuration.

3.2.101. TLS/SSL Server is enabling the BEAST attack (ssl-cve-2011-3389-beast)*Description:*

The SSL protocol, as used in certain configurations of Microsoft Windows and browsers such as Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera (and other products negotiating SSL connections) encrypts data by using CBC mode with chained initialization vectors. This potentially allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack. By supporting the affected protocols and ciphers, the server is enabling the clients in to being exploited.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
172.16.1.12:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_DES_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA
172.16.1.156:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.0 ciphers: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
172.16.1.156:3389	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
172.16.1.180:8181	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Affected Nodes:	Additional Information:
	<p>TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA</p> <p>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA</p> <p>TLS_RSA_WITH_3DES_EDE_CBC_SHA</p> <p>TLS_RSA_WITH_AES_128_CBC_SHA</p>
172.16.1.25:8181	<p>Negotiated with the following insecure cipher suites: TLS 1.0 ciphers:</p> <p>TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA</p> <p>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</p> <p>TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA</p> <p>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA</p> <p>TLS_RSA_WITH_3DES_EDE_CBC_SHA</p> <p>TLS_RSA_WITH_AES_128_CBC_SHA</p>
172.16.1.46:5989	<p>Negotiated with the following insecure cipher suites: SSL 3.0 ciphers:</p> <p>TLS_RSA_WITH_3DES_EDE_CBC_SHA</p> <p>TLS_RSA_WITH_AES_128_CBC_SHA</p> <p>TLS_RSA_WITH_AES_256_CBC_SHA</p> <p>TLS_RSA_WITH_DES_CBC_SHA</p> <p>TLS 1.0 ciphers:</p> <p>TLS_RSA_WITH_3DES_EDE_CBC_SHA</p> <p>TLS_RSA_WITH_AES_128_CBC_SHA</p> <p>TLS_RSA_WITH_AES_256_CBC_SHA</p> <p>TLS_RSA_WITH_DES_CBC_SHA</p>
172.16.1.7:443	<p>Negotiated with the following insecure cipher suites: SSL 3.0 ciphers:</p> <p>TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA</p> <p>TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA</p> <p>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</p> <p>TLS_DHE_RSA_WITH_AES_256_CBC_SHA</p> <p>TLS_DHE_RSA_WITH_DES_CBC_SHA</p> <p>TLS_RSA_EXPORT_WITH_DES40_CBC_SHA</p> <p>TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5</p> <p>TLS_RSA_WITH_3DES_EDE_CBC_SHA</p> <p>TLS_RSA_WITH_AES_128_CBC_SHA</p> <p>TLS_RSA_WITH_AES_256_CBC_SHA</p> <p>TLS_RSA_WITH_DES_CBC_SHA</p> <p>TLS 1.0 ciphers:</p> <p>TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA</p> <p>TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA</p> <p>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</p> <p>TLS_DHE_RSA_WITH_AES_256_CBC_SHA</p> <p>TLS_DHE_RSA_WITH_DES_CBC_SHA</p> <p>TLS_RSA_EXPORT_WITH_DES40_CBC_SHA</p> <p>TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5</p> <p>TLS_RSA_WITH_3DES_EDE_CBC_SHA</p> <p>TLS_RSA_WITH_AES_128_CBC_SHA</p> <p>TLS_RSA_WITH_AES_256_CBC_SHA</p> <p>TLS_RSA_WITH_DES_CBC_SHA</p>

References:

Source	Reference
CVE	CVE-2011-3389
URL	http://vnhacker.blogspot.co.uk/2011/09/beast.html

Vulnerability Solution:

There is no server-side mitigation available against the BEAST attack. The only option is to disable the affected protocols (SSLv3 and TLS 1.0). The only fully safe configuration is to use Authenticated Encryption with Associated Data (AEAD), e.g. AES-GCM, AES-CCM in TLS 1.2.

3.2.102. Cross-protocol attack on TLS using SSLv2 (DROWN) (CVE-2016-0800) (ssl-cve-2016-0800)*Description:*

The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.7:443	Successfully connected to 172.16.1.7:443 over SSLv2 using a vulnerable cipher

References:

Source	Reference
CVE	CVE-2016-0800
URL	https://access.redhat.com/articles/2176731

Vulnerability Solution:

Configure the server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.

3.2.103. Self-signed TLS/SSL certificate (ssl-self-signed-certificate)*Description:*

The server's TLS/SSL certificate is self-signed. Self-signed certificates cannot be trusted by default, especially because TLS/SSL man-in-the-middle attacks typically use self-signed certificates to eavesdrop on TLS/SSL connections.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:443	TLS/SSL certificate is self-signed.
172.16.1.180:8181	TLS/SSL certificate is self-signed.
172.16.1.25:8181	TLS/SSL certificate is self-signed.
172.16.1.46:5989	TLS/SSL certificate is self-signed.

References:

None

Vulnerability Solution:

Obtain a new TLS/SSL server certificate that is NOT self-signed and install it on the server. The exact instructions for obtaining a new certificate depend on your organization's requirements. Generally, you will need to generate a certificate request and save the request as a file. This file is then sent to a Certificate Authority (CA) for processing. Your organization may have its own internal Certificate Authority. If not, you may have to pay for a certificate from a trusted external Certificate Authority, such as [Thawte](#) or [Verisign](#).

3.2.104. TLS/SSL Server is enabling the POODLE attack (sslv3-cve-2014-3566-poodle)*Description:*

All systems and applications utilizing the Secure Socket Layer (SSL) 3.0 with cipher-block chaining (CBC) mode ciphers may be vulnerable to POODLE (Padding Oracle On Downgraded Legacy Encryption) attacks. The SSL 3.0 vulnerability stems from the way blocks of data are encrypted under a specific type of encryption algorithm within the SSL protocol. The POODLE attack takes advantage of the protocol version negotiation feature built into SSL to force the use of SSL 3.0 and then leverages this new vulnerability to decrypt select content within the SSL session.

The Payment Card Industry (PCI) Data Security Standard requires a minimum of TLS v1.1 and recommends TLS v1.2. In addition, FIPS 140-2 standard also requires a minimum of TLS v1.1 and recommends TLS v1.2.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_DES_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA
172.16.1.156:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA
172.16.1.46:5989	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA
172.16.1.7:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_DES_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA

Affected Nodes:	Additional Information:
	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA

References:

Source	Reference
CVE	CVE-2014-3566
URL	https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf
URL	https://www.us-cert.gov/ncas/alerts/TA14-290A

Vulnerability Solution:

Configure the server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.

3.2.105. TLS/SSL Server Supports SSLv3 (ssl3-supported)*Description:*

The SSLv3 protocol and supported ciphers all suffer from serious vulnerabilities making this protocol unsafe to use.

The Payment Card Industry (PCI) Data Security Standard requires a minimum of TLS v1.1 and recommends TLS v1.2. In addition, FIPS 140-2 standard also requires a minimum of TLS v1.1 and recommends TLS v1.2.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:443	Successfully connected over SSLv3
172.16.1.156:443	Successfully connected over SSLv3
172.16.1.46:5989	Successfully connected over SSLv3
172.16.1.7:443	Successfully connected over SSLv3

References:

Source	Reference
CVE	CVE-2014-3566
URL	https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

Vulnerability Solution:

Configure the server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.

3.2.106. Diffie-Hellman group smaller than 1024 bits (tls-dh-prime-under-1024-bits)*Description:*

The TLS server uses a Diffie-Hellman group with a prime modulus of less than 1024 bits in length. Current estimates are that that an academic team can break a 768-bit prime and that a state-level actor can break a 1024-bit prime.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:443	The following SSL/TLS cipher suites use Diffie-Hellman a prime modulus smaller than 1024 bits:SSL 3.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA with a Diffie-Hellman prime modulus of 512 bits
172.16.1.25:8181	The following SSL/TLS cipher suites use Diffie-Hellman a prime modulus smaller than 1024 bits:TLS 1.0 ciphers: TLS_DHE_RSA_WITH_AES_128_CBC_SHA with a Diffie-Hellman prime modulus of 768 bitsTLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA with a Diffie-Hellman prime modulus of 768 bits
172.16.1.7:443	The following SSL/TLS cipher suites use Diffie-Hellman a prime modulus smaller than 1024 bits:SSL 3.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA with a Diffie-Hellman prime modulus of 512 bitsTLS 1.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA with a Diffie-Hellman prime modulus of 512 bits

References:

Source	Reference
URL	https://weakdh.org/

Vulnerability Solution:

Please refer to this [guide to deploying Diffie-Hellman for TLS](#) for instructions on how to configure the server to use 2048-bit or stronger Diffie-Hellman groups with safe primes.

3.2.107. TLS Server Supports DHE_EXPORT Cipher Algorithms (CVE-2015-4000) (tls-dhe-export-ciphers-cve-2015-4000)*Description:*

The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a

ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
172.16.1.7:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS 1.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA

References:

Source	Reference
CVE	CVE-2015-4000
URL	https://weakdh.org/

Vulnerability Solution:

Configure the server to disable support for export ciphers.

For Microsoft IIS web servers, see Microsoft Knowledgebase article [245030](#) for instructions on disabling export ciphers.

The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.

Refer to your server vendor documentation to apply the recommended cipher configuration:

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

3.2.108. TLS Server Supports TLS version 1.0 (tlsv1_0-enabled)

Description:

The PCI (Payment Card Industry) Data Security Standard requires a minimum of TLS v1.1 and recommends TLS v1.2. In addition, FIPS 140-2 standard requires a minimum of TLS v1.1 and recommends TLS v1.2.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Successfully connected over TLSv1.0
172.16.1.156:443	Successfully connected over TLSv1.0

Affected Nodes:	Additional Information:
172.16.1.156:3389	Successfully connected over TLSv1.0
172.16.1.180:8181	Successfully connected over TLSv1.0
172.16.1.25:8181	Successfully connected over TLSv1.0
172.16.1.46:5989	Successfully connected over TLSv1.0
172.16.1.7:443	Successfully connected over TLSv1.0

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

Vulnerability Solution:

Configure the server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.

3.2.109. Unencrypted X11 Service Available (x11-open-port)*Description:*

XWindows is an unencrypted protocol, as such it sends sensitive data in clear text.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.7:6000	Running XWindows service

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

Vulnerability Solution:

Stop the X Server from listening on TCP ports, ensure it is running with: `-nolisten tcp`
 Replace it with other technologies like SSH with X-forwarding.

3.3. Moderate Vulnerabilities**3.3.1. HTTP OPTIONS Method Enabled (http-options-method-enabled)***Description:*

Web servers that respond to the OPTIONS HTTP method expose what other methods are supported by the web server, allowing attackers to narrow and intensify their efforts.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.156:80	OPTIONS method returned values including itself
172.16.1.180:80	OPTIONS method returned values including itself
172.16.1.180:8080	OPTIONS method returned values including itself
172.16.1.180:8181	OPTIONS method returned values including itself
172.16.1.25:8181	OPTIONS method returned values including itself
172.16.1.7:80	OPTIONS method returned values including itself
172.16.1.7:443	OPTIONS method returned values including itself
172.16.1.7:631	OPTIONS method returned values including itself
172.16.1.7:7778	OPTIONS method returned values including itself
172.16.1.7:8008	OPTIONS method returned values including itself
181.118.158.2:8443	OPTIONS method returned values including itself

References:

Source	Reference
URL	https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Vulnerability Solution:

•Disable HTTP OPTIONS method

Disable HTTP OPTIONS method on your web server. Refer to your web server's instruction manual on how to do this.

Web servers that respond to the OPTIONS HTTP method expose what other methods are supported by the web server, allowing attackers to narrow and intensify their efforts.

•Apache HTTPD

Disable HTTP OPTIONS Method for Apache

Disable the OPTIONS method by including the following in the Apache configuration:

```
<Limit OPTIONS>
Order deny,allow
Deny from all
</Limit>
```

•Microsoft IIS

Disable HTTP OPTIONS Method for IIS

Disable the OPTIONS method by doing the following in the IIS manager

1. Select relevant site
2. Select Request filtering and change to HTTP verb tab
3. Select Deny Verb from the actions pane
4. Type OPTIONS into the provided text box and press OK

•nginx nginx

Disable HTTP OPTIONS Method for nginx

Disable the OPTIONS method by adding the following line to your server block, you can add other HTTP methods to be allowed to run after POST

```
limit_except GET POST { deny all; }
```

3.3.2. SSH CBC vulnerability (ssh-cbc-ciphers)

Description:

SSH contains a vulnerability in the way certain types of errors are handled. Attacks leveraging this vulnerability would lead to the loss of the SSH session. According to CPNI Vulnerability Advisory SSH:

If exploited, this attack can potentially allow an attacker to recover up to 32 bits of plaintext from an arbitrary block of ciphertext from a connection secured using the SSH protocol in the standard configuration. If OpenSSH is used in the standard configuration, then the attacker's success probability for recovering 32 bits of plaintext is 2^{-18} . A variant of the attack against OpenSSH in the standard configuration can verifiably recover 14 bits of plaintext with probability 2^{-14} . The success probability of the attack for other implementations of SSH is not known.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:22	Running SSH serviceInsecure CBC ciphers in use: aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc
172.16.1.103:22	Running SSH serviceInsecure CBC ciphers in use: aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc
172.16.1.111:22	Running SSH serviceInsecure CBC ciphers in use: aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc
172.16.1.12:22	Running SSH serviceInsecure CBC ciphers in use: aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc
172.16.1.46:22	Running SSH serviceInsecure CBC ciphers in use: aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc
172.16.1.7:22	Running SSH serviceInsecure CBC ciphers in use: aes128-cbc,3des-

Affected Nodes:	Additional Information:
	cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc

References:

Source	Reference
URL	https://www.kb.cert.org/vuls/id/958563

Vulnerability Solution:

SSH can be done using Counter (CTR) mode encryption. This mode generates the keystream by encrypting successive values of a "counter" function. In order to mitigate this vulnerability SSH can be setup to use CTR mode rather CBC mode.

3.3.3. OpenSSH CBC Mode Information Disclosure Vulnerability (ssh-openssh-cbc-mode-info-disclosure)*Description:*

Error handling in the SSH protocol in (1) SSH Tectia Client and Server and Connector 4.0 through 4.4.11, 5.0 through 5.2.4, and 5.3 through 5.3.8; Client and Server and ConnectSecure 6.0 through 6.0.4; Server for Linux on IBM System z 6.0.4; Server for IBM z/OS 5.5.1 and earlier, 6.0.0, and 6.0.1; and Client 4.0-J through 4.3.3-J and 4.0-K through 4.3.10-K; and (2) OpenSSH 4.7p1 and possibly other versions, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.7:22	OpenBSD OpenSSH 4.3 on Linux 2.6.18

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
BID	32319
CERT-VN	958563
CVE	CVE-2008-5161
OVAL	11279
REDHAT	RHSA-2009:1287
URL	http://www.ssh.com/company/news/article/953/
XF	46620

Vulnerability Solution:

OpenBSD OpenSSH < 5.2

Download and apply the upgrade from: <ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH>

While you can always [build OpenSSH from source](#), many platforms and distributions provide pre-built binary packages for OpenSSH. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the

packages if they are available for your operating system.

3.3.4. TLS/SSL Server Supports The Use of Static Key Ciphers (ssl-static-key-ciphers)

Description:

The server is configured to support ciphers known as static key ciphers. These ciphers don't support "Forward Secrecy". In the new specification for HTTP/2, these ciphers have been blacklisted.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA TLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA TLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
172.16.1.12:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5 TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA
172.16.1.156:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA

Affected Nodes:	Additional Information:
	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA
172.16.1.156:3389	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA
172.16.1.180:8181	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256
172.16.1.25:8181	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA
172.16.1.46:5989	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA
172.16.1.7:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers:

Affected Nodes:	Additional Information:
	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5 TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS 1.0 ciphers: TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5 TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA
181.118.158.2:8443	Negotiated with the following insecure cipher suites: TLS 1.1 ciphers: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA TLS 1.2 ciphers: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_CCM TLS_RSA_WITH_AES_128_CCM_8 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_256_CCM TLS_RSA_WITH_AES_256_CCM_8 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256

References:

Source	Reference
URL	http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295
URL	https://wiki.mozilla.org/Security/Server_Side_TLS
URL	https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Rule_-_Only_Support_Strong_Cryptographic_Ciphers
URL	http://support.microsoft.com/kb/245030/
URL	https://tools.ietf.org/html/rfc7540/

Vulnerability Solution:

Configure the server to disable support for static key cipher suites.

For Microsoft IIS web servers, see Microsoft Knowledgebase article [245030](http://support.microsoft.com/kb/245030/) for instructions on disabling static key cipher suites.

The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use

TLSv1.1 and TLSv1.2 protocols.

Refer to your server vendor documentation to apply the recommended cipher configuration:

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

3.3.5. Diffie-Hellman group smaller than 2048 bits (tls-dh-prime-under-2048-bits)

Description:

The TLS server uses a Diffie-Hellman group with a prime modulus of less than 2048 bits in length. Current estimates are that that an academic team can break a 768-bit prime and that a state-level actor can break a 1024-bit prime.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:443	The following SSL/TLS cipher suites use Diffie-Hellman a prime modulus smaller than 2048 bits:SSL 3.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA with a Diffie-Hellman prime modulus of 512 bitsTLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bits
172.16.1.180:8181	The following SSL/TLS cipher suites use Diffie-Hellman a prime modulus smaller than 2048 bits:TLS 1.0 ciphers: TLS_DHE_RSA_WITH_AES_128_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bitsTLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bitsTLS 1.1 ciphers: TLS_DHE_RSA_WITH_AES_128_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bitsTLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bits
172.16.1.25:8181	The following SSL/TLS cipher suites use Diffie-Hellman a prime modulus smaller than 2048 bits:TLS 1.0 ciphers: TLS_DHE_RSA_WITH_AES_128_CBC_SHA with a Diffie-Hellman prime modulus of 768 bitsTLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA with a Diffie-Hellman prime modulus of 768 bits
172.16.1.7:443	The following SSL/TLS cipher suites use Diffie-Hellman a prime modulus smaller than 2048 bits:SSL 3.0 ciphers: TLS_DHE_RSA_WITH_AES_128_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bitsTLS_DHE_RSA_WITH_AES_256_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bits TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA with a Diffie-Hellman prime modulus of 512 bitsTLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bitsTLS 1.0 ciphers:

Affected Nodes:	Additional Information:
	<p>TLS_DHE_RSA_WITH_AES_128_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bits</p> <p>TLS_DHE_RSA_WITH_AES_256_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bits</p> <p>TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA with a Diffie-Hellman prime modulus of 512 bits</p> <p>TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bits</p>

References:

Source	Reference
URL	https://weakdh.org/

Vulnerability Solution:

Please refer to this [guide to deploying Diffie-Hellman for TLS](#) for instructions on how to configure the server to use 2048-bit or stronger Diffie-Hellman groups with safe primes.

3.3.6. TLS/SSL Server Is Using Commonly Used Prime Numbers (tls-dh-primes)*Description:*

The server is using a common or default prime number as a parameter during the Diffie-Hellman key exchange. This makes the secure session vulnerable to a precomputation attack. An attacker can spend a significant amount of time to generate a lookup/rainbow table for a particular prime number. This lookup table can then be used to obtain the shared secret for the handshake and decrypt the session.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	<p>The server is using the following commonly used Diffie-Hellman primes:</p> <pre> ffffffffffffc90fdaa22168c234c4c6628b80dc1cd129024e088a67cc74020bbea63 b139b22514a08798e3404ddef9519b3cd3a431b302b0a6df25f14374fe1356d6d5 1c245e485b576625e7ec6f44c42e9a637ed6b0bff5cb6f406b7edee386bfb5a899f a5ae9f24117c4b1fe649286651ece45b3dc2007cb8a163bf0598da48361c55d39 a69163fa8fd24cf5f83655d23dca3ad961c62f356208552bb9ed529077096966d6 70c354e4abc9804f1746c08ca18217c32905e462e36ce3be39e772c180e86039b 2783a2ec07a28fb5c55df06f4c52c9de2bcbf6955817183995497cea956ae515d2 261898fa051015728e5a8aaca68ffffffffffffff </pre>
172.16.1.12:443	<p>The server is using the following commonly used Diffie-Hellman primes:</p> <pre> fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455 d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950 a5a49f9fe8047b1022c24fba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51e c3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7 fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f 35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17 </pre>
172.16.1.180:8181	<p>The server is using the following commonly used Diffie-Hellman primes:</p>

Affected Nodes:	Additional Information:
	ffffffffffffc90fdaa22168c234c4c6628b80dc1cd129024e088a67cc74020bba63b139b22514a08798e3404ddef9519b3cd3a431b302b0a6df25f14374fe1356d6d51c245e485b576625e7ec6f44c42e9a637ed6b0bff5cb6f406b7edee386bfb5a899fa5ae9f24117c4b1fe649286651ece65381ffffffffffff
172.16.1.25:8181	The server is using the following commonly used Diffie-Hellman primes: e9e642599d355f37c97fd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf
172.16.1.7:443	The server is using the following commonly used Diffie-Hellman primes: e6969d3d495be32c7cf180c3bdd4798e91b7818251bb055e2a2064904a79a770fa15a259cbd523a6a6ef09c43048d5a22f971f3c20129b48000e6edd061cbc053e371d794e5327df611ebbbe1bac9b5c6044cf023d76e05eea9bad991b13a63c974e9ef1839eb5db125136f7262e56a8871538dfd823c6505085e21f0dd5c86bd4bcd52406f69b35994b88de5db89682c8157f62d8f33633ee5772f11f05ab22d6b5145b9f241e5acc31ff090a4bc71148976f76795094e71e7903529f5a824b
181.118.158.2:8443	The server is using the following commonly used Diffie-Hellman primes: ffffffffffffc90fdaa22168c234c4c6628b80dc1cd129024e088a67cc74020bba63b139b22514a08798e3404ddef9519b3cd3a431b302b0a6df25f14374fe1356d6d51c245e485b576625e7ec6f44c42e9a637ed6b0bff5cb6f406b7edee386bfb5a899fa5ae9f24117c4b1fe649286651ece45b3dc2007cb8a163bf0598da48361c55d39a69163fa8fd24cf5f83655d23dca3ad961c62f356208552bb9ed529077096966d670c354e4abc9804f1746c08ca18217c32905e462e36ce3be39e772c180e86039b2783a2ec07a28fb5c55df06f4c52c9de2bcbf6955817183995497cea956ae515d2261898fa051015728e5a8aaca68ffffffffffff

References:

Source	Reference
URL	https://weakdh.org/
URL	https://www.openssl.org/docs/man1.1.0/apps/dhparam.html

Vulnerability Solution:

Configure the server to use a randomly generated Diffie-Hellman group. It's recommend that you generate a 2048-bit group. The simplest way of generating a new group is to use OpenSSL:

```
openssl dhparam -out dhparams.pem 2048
```

To use the DH parameters in newer versions of Apache (2.4.8 and newer) and OpenSSL 1.0.2 or later, you can directly specify your DH params file as follows:

```
SSLOpenSSLConfCmd DHParameters "{path to dhparams.pem}"
```

If you are using Apache with LibreSSL, or Apache 2.4.7 and OpenSSL 0.9.8a or later, you can append the DHparams you generated earlier to the end of your certificate file and reload the configuration.

For other products see [the remediation steps suggested by the original researchers](#).

3.3.7. SHA-1-based Signature in TLS/SSL Server X.509 Certificate (tls-server-cert-sig-sha1)

Description:

The SHA-1 hashing algorithm has known weaknesses that expose it to collision attacks, which may allow an attacker to generate additional X.509 digital certificates with the same signature as an original.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.7:443	SSL certificate is signed with SHA1withRSA

References:

Source	Reference
URL	https://technet.microsoft.com/en-us/library/security/2880823.aspx
URL	https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/
URL	http://googleonlinesecurity.blogspot.co.uk/2014/09/gradually-sunsetting-sha-1.html
URL	https://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html

Vulnerability Solution:

Stop using signature algorithms relying on SHA-1, such as "SHA1withRSA", when signing X.509 certificates. Instead, use the SHA-2 family (SHA-224, SHA-256, SHA-384, and SHA-512).

3.3.8. TLS Server Supports TLS version 1.1 (tlsv1_1-enabled)

Description:

The PCI (Payment Card Industry) Data Security Standard requires a minimum of TLS v1.1 and recommends TLS v1.2. In addition, FIPS 140-2 standard requires a minimum of TLS v1.1 and recommends TLS v1.2.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Successfully connected over TLSv1.1
172.16.1.156:443	Successfully connected over TLSv1.1
172.16.1.156:3389	Successfully connected over TLSv1.1
172.16.1.180:8181	Successfully connected over TLSv1.1
181.118.158.2:8443	Successfully connected over TLSv1.1

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf

Source	Reference
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

Vulnerability Solution:

Configure the server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.

3.3.9. Weak Cryptographic Key (weak-crypto-key)*Description:*

The key length used by a cryptographic algorithm determines the highest security it can offer. Newly discovered theoretical attacks and hardware advances constantly erode this security level over time. Taking this into account, as of 2011, governmental, academic, and private organizations providing guidance on cryptographic security, such as the [National Institute of Standards and Technology](#) (NIST), the [European Network of Excellence in Cryptology II](#) (ECRYPT II), make the following general recommendations to provide short to medium term security against even the most well-funded attackers (eg. intelligence agencies):

- Symmetric key lengths of at least 80-112 bits.
- Elliptic curve key lengths of at least 160-224 bits.
- RSA key lengths of at least 1248-2048 bits. In particular, the CA/Browser Forum [Extended Validation \(EV\) Guidelines](#) require a minimum key length of 2048 bits. Also, current research shows that factoring a 1024-bit RSA modulus [is within practical reach](#).
- DSA key lengths of at least 2048 bits.

Additionally, starting in 2014, the Certificate Authority/Browser Forum has mandated that 1024-bit RSA keys no longer be supported for SSL certificates or code signing.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:443	Length of RSA modulus in X.509 certificate: 1024 bits (less than 2047 bits)
172.16.1.7:443	Length of RSA modulus in X.509 certificate: 1024 bits (less than 2047 bits)

References:

Source	Reference
URL	http://csrc.nist.gov/groups/ST/toolkit/key_management.html
URL	http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf
URL	http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/QES/Veroeffentlichung/en/Algorithmen/2011_2_AlgoKatpdf.pdf
URL	http://www.ecrypt.eu.org/documents/D.SPA.17.pdf
URL	http://www.keylength.com
URL	http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf

Source	Reference
URL	http://www.symantec.com/page.jsp?id=1024-bit-certificate-support

Vulnerability Solution:

If the weak key is used in an X.509 certificate (for example for an HTTPS server), generate a longer key and recreate the certificate. Please also refer to [NIST's recommendations on cryptographic algorithms and key lengths](#).

3.3.10. PHP Vulnerability: CVE-2018-10545 (php-cve-2018-10545)*Description:*

An issue was discovered in PHP before 5.6.35, 7.0.x before 7.0.29, 7.1.x before 7.1.16, and 7.2.x before 7.2.4. Dumpable FPM child processes allow bypassing opcache access controls because fpm_unix.c makes a PR_SET_DUMPABLE prctl call, allowing one user (in a multiuser environment) to obtain sensitive information from the process memory of a second user's PHP applications by running gcore on the PID of the PHP-FPM worker process.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Running HTTPS serviceProduct HTTPD exists -- Apache HTTPDVulnerable version of component PHP found -- PHP 7.1.8

References:

Source	Reference
BID	104022
CVE	CVE-2018-10545
DEBIAN	DSA-4240
REDHAT	RHSA-2019:2519
URL	https://bugs.php.net/bug.php?id=75605

Vulnerability Solution:

- Upgrade to PHP version 5.6.35
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.0.29
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.1.16
Download and apply the upgrade from: <http://www.php.net/releases/>
- Upgrade to PHP version 7.2.4
Download and apply the upgrade from: <http://www.php.net/releases/>

3.3.11. ICMP timestamp response (generic-icmp-timestamp)

Description:

The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services.

In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1	Able to determine remote system time.
172.16.1.103	Able to determine remote system time.
172.16.1.111	Able to determine remote system time.
172.16.1.12	Able to determine remote system time.
172.16.1.156	Able to determine remote system time.
172.16.1.180	Able to determine remote system time.
172.16.1.25	Able to determine remote system time.
172.16.1.46	Able to determine remote system time.
172.16.1.7	Able to determine remote system time.

References:

Source	Reference
CVE	CVE-1999-0524
OSVDB	95
XF	306
XF	322

Vulnerability Solution:

•HP-UX

Disable ICMP timestamp responses on HP/UX

Execute the following command:

```
ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Cisco IOS

Disable ICMP timestamp responses on Cisco IOS

Use ACLs to block ICMP types 13 and 14. For example:

```
deny icmp any any 13
```

```
deny icmp any any 14
```

Note that it is generally preferable to use ACLs that block everything by default and then selectively allow certain types of traffic in. For example, block everything and then only allow ICMP unreachable, ICMP echo reply, ICMP time exceeded, and ICMP source quench:

```
permit icmp any any unreachable
```

```
permit icmp any any echo-reply
```

```
permit icmp any any time-exceeded
```

```
permit icmp any any source-quench
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•SGI Irix

Disable ICMP timestamp responses on SGI Irix

IRIX does not offer a way to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using `ipfilterd`, and/or block it at any external firewalls.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Linux

Disable ICMP timestamp responses on Linux

Linux offers neither a `sysctl` nor a `/proc/sys/net/ipv4` interface to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using `iptables`, and/or block it at the firewall. For example:

```
ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
```

```
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition

Disable ICMP timestamp responses on Windows NT 4

Windows NT 4 does not provide a way to block ICMP packets. Therefore, you should block them at the firewall.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•OpenBSD

Disable ICMP timestamp responses on OpenBSD

Set the "net.inet.icmp.tstamprepl" `sysctl` variable to 0.

```
sysctl -w net.inet.icmp.tstamprepl=0
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

- Cisco PIX

Disable ICMP timestamp responses on Cisco PIX

A properly configured PIX firewall should never respond to ICMP packets on its external interface. In PIX Software versions 4.1(6) until 5.2.1, ICMP traffic to the PIX's internal interface is permitted; the PIX cannot be configured to NOT respond. Beginning in PIX Software version 5.2.1, ICMP is still permitted on the internal interface by default, but ICMP responses from its internal interfaces can be disabled with the `icmp deny any 13 <inside>` command, as follows, where `<inside>` is the name of the internal interface:

```
icmp deny any 13 <inside>
```

```
icmp deny any 14 <inside>
```

Don't forget to save the configuration when you are finished.

See Cisco's support document [Handling ICMP Pings with the PIX Firewall](#) for more information.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

- Sun Solaris

Disable ICMP timestamp responses on Solaris

Execute the following commands:

```
/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp 0
```

```
/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

- Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server

Disable ICMP timestamp responses on Windows 2000

Use the IPsec filter feature to define and apply an IP filter list that blocks ICMP types 13 and 14. Note that the standard TCP/IP blocking capability under the "Networking and Dialup Connections" control panel is NOT capable of blocking ICMP (only TCP and UDP). The IPsec filter features, while they may seem strictly related to the IPsec standards, will allow you to selectively block these ICMP packets. See <http://support.microsoft.com/kb/313190> for more information.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

- Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003

Disable ICMP timestamp responses on Windows XP/2K3

ICMP timestamp responses can be disabled by deselecting the "allow incoming timestamp request" option in the ICMP configuration panel of Windows Firewall.

1. Go to the Network Connections control panel.
2. Right click on the network adapter and select "properties", or select the internet adapter and select File->Properties.
3. Select the "Advanced" tab.
4. In the Windows Firewall box, select "Settings".

5. Select the "General" tab.
6. Enable the firewall by selecting the "on (recommended)" option.
7. Select the "Advanced" tab.
8. In the ICMP box, select "Settings".
9. Deselect (uncheck) the "Allow incoming timestamp request" option.
10. Select "OK" to exit the ICMP Settings dialog and save the settings.
11. Select "OK" to exit the Windows Firewall dialog and save the settings.
12. Select "OK" to exit the internet adapter dialog.

For more information, see: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true

•Microsoft Windows Vista, Microsoft Windows Vista Home, Basic Edition, Microsoft Windows Vista Home, Basic N Edition, Microsoft Windows Vista Home, Premium Edition, Microsoft Windows Vista Ultimate Edition, Microsoft Windows Vista Enterprise Edition, Microsoft Windows Vista Business Edition, Microsoft Windows Vista Business N Edition, Microsoft Windows Vista Starter Edition, Microsoft Windows Server 2008, Microsoft Windows Server 2008 Standard Edition, Microsoft Windows Server 2008 Enterprise Edition, Microsoft Windows Server 2008 Datacenter Edition, Microsoft Windows Server 2008 HPC Edition, Microsoft Windows Server 2008 Web Edition, Microsoft Windows Server 2008 Storage Edition, Microsoft Windows Small Business Server 2008, Microsoft Windows Essential Business Server 2008

Disable ICMP timestamp responses on Windows Vista/2008

ICMP timestamp responses can be disabled via the netsh command line utility.

1. Go to the Windows Control Panel.
2. Select "Windows Firewall".
3. In the Windows Firewall box, select "Change Settings".
4. Enable the firewall by selecting the "on (recommended)" option.
5. Open a Command Prompt.
6. Enter "netsh firewall set icmpsetting 13 disable"

For more information, see: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true

•Disable ICMP timestamp responses

Disable ICMP timestamp replies for the device. If the device does not support this level of configuration, the easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

3.3.12. TCP timestamp response (generic-tcp-timestamp)

Description:

The remote host responded with a TCP timestamp. The TCP timestamp response can be used to approximate the remote host's uptime, potentially aiding in further attacks. Additionally, some operating systems can be fingerprinted based on the behavior of their TCP timestamps.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1	Able to determine system boot time.
172.16.1.180	Able to determine system boot time.
181.118.158.2	Able to determine system boot time.

References:

Source	Reference
URL	http://uptime.netcraft.com
URL	http://www.forensicswiki.org/wiki/TCP_timestamps
URL	http://www.ietf.org/rfc/rfc1323.txt

Vulnerability Solution:

•Cisco

Disable TCP timestamp responses on Cisco

Run the following command to disable TCP timestamps:

```
no ip tcp timestamp
```

•FreeBSD

Disable TCP timestamp responses on FreeBSD

Set the value of net.inet.tcp.rfc1323 to 0 by running the following command:

```
sysctl -w net.inet.tcp.rfc1323=0
```

Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:

```
net.inet.tcp.rfc1323=0
```

•Linux

Disable TCP timestamp responses on Linux

Set the value of net.ipv4.tcp_timestamps to 0 by running the following command:

```
sysctl -w net.ipv4.tcp_timestamps=0
```

Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:

```
net.ipv4.tcp_timestamps=0
```

- OpenBSD

Disable TCP timestamp responses on OpenBSD

Set the value of net.inet.tcp.rfc1323 to 0 by running the following command:

```
sysctl -w net.inet.tcp.rfc1323=0
```

Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:

```
net.inet.tcp.rfc1323=0
```

- Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition, Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows 98SE, Microsoft Windows ME, Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server, Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows XP Tablet PC Edition, Microsoft Windows CE, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003, Microsoft Windows Server 2003 R2, Microsoft Windows Server 2003 R2, Standard Edition, Microsoft Windows Server 2003 R2, Enterprise Edition, Microsoft Windows Server 2003 R2, Datacenter Edition, Microsoft Windows Server 2003 R2, Web Edition, Microsoft Windows Small Business Server 2003 R2, Microsoft Windows Server 2003 R2, Express Edition, Microsoft Windows Server 2003 R2, Workgroup Edition

Disable TCP timestamp responses on Windows versions before Vista

Set the Tcp1323Opts value in the following key to 1:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

- Microsoft Windows Server 2008, Microsoft Windows Server 2008 Standard Edition, Microsoft Windows Server 2008 Enterprise Edition, Microsoft Windows Server 2008 Datacenter Edition, Microsoft Windows Server 2008 HPC Edition, Microsoft Windows Server 2008 Web Edition, Microsoft Windows Server 2008 Storage Edition, Microsoft Windows Small Business Server 2008, Microsoft Windows Essential Business Server 2008, Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 R2, Standard Edition, Microsoft Windows Server 2008 R2, Enterprise Edition, Microsoft Windows Server 2008 R2, Datacenter Edition, Microsoft Windows Server 2008 R2, Web Edition, Microsoft Windows Server 2012, Microsoft Windows Server 2012 Standard Edition, Microsoft Windows Server 2012 Foundation Edition, Microsoft Windows Server 2012 Essentials Edition, Microsoft Windows Server 2012 Datacenter Edition, Microsoft Windows Storage Server 2012, Microsoft Windows Vista, Microsoft Windows Vista Home, Basic Edition, Microsoft Windows Vista Home, Basic N Edition, Microsoft Windows Vista Home, Premium Edition, Microsoft Windows Vista Ultimate Edition, Microsoft

Windows Vista Enterprise Edition, Microsoft Windows Vista Business Edition, Microsoft Windows Vista Business N Edition, Microsoft Windows Vista Starter Edition, Microsoft Windows 7, Microsoft Windows 7 Home, Basic Edition, Microsoft Windows 7 Home, Basic N Edition, Microsoft Windows 7 Home, Premium Edition, Microsoft Windows 7 Home, Premium N Edition, Microsoft Windows 7 Ultimate Edition, Microsoft Windows 7 Ultimate N Edition, Microsoft Windows 7 Enterprise Edition, Microsoft Windows 7 Enterprise N Edition, Microsoft Windows 7 Professional Edition, Microsoft Windows 7 Starter Edition, Microsoft Windows 7 Starter N Edition, Microsoft Windows 8, Microsoft Windows 8 Enterprise Edition, Microsoft Windows 8 Professional Edition, Microsoft Windows 8 RT, Microsoft Windows Longhorn Server Beta

Disable TCP timestamp responses on Windows versions since Vista

TCP timestamps cannot be reliably disabled on this OS. If TCP timestamps present enough of a risk, put a firewall capable of blocking TCP timestamp packets in front of the affected assets.

3.3.13. NetBIOS NBSTAT Traffic Amplification ([netbios-nbstat-amplification](#))

Description:

A NetBIOS NBSTAT query will obtain the status from a NetBIOS-speaking endpoint, which will include any names that the endpoint is known to respond to as well as the device's MAC address for that endpoint. A NBSTAT response is roughly 3x the size of the request, and because NetBIOS utilizes UDP, this can be used to conduct traffic amplification attacks against other assets, typically in the form of distributed reflected denial of service (DRDoS) attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.156:137	Running CIFS Name Service serviceConfiguration item advertised-name-count set to '3' matched
172.16.1.7:137	Running CIFS Name Service serviceConfiguration item advertised-name-count set to '7' matched

References:

Source	Reference
CERT	TA14-017A

Vulnerability Solution:

NetBIOS can be important to the proper functioning of a Windows network depending on the design. Restrict access to the NetBIOS service to only trusted assets.

3.3.14. NTP clock variables information disclosure ([ntp-clock-variables-disclosure](#))

Description:

This sytem allows the internal NTP variables to be queried. These variables contain potentially sensitive information, such as the NTP software version, operating system version, peers, and more.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:123	The following NTP variables were found from a readvar request: clock, error, freq, leap, peer, phase, poll, refid, reftime, rootdelay, rootdispersion, stratum, system

References:

None

Vulnerability Solution:

•Disable NTP queries

Apply a restrict option to all hosts that are not authorized to perform NTP queries. For example, to deny query requests from all clients, put the following in the NTP configuration file, typically /etc/ntp.conf, and restart the NTP service:

```
restrict default nomodify nopeer noquery notrap
```

•Cisco

Restrict NTP readvar queries

Apply an ACL that restricts NTP readvar queries from unauthorized clients, as described in the ['Configuring an NTP Access Group' section of the Cisco IOS documentation](#).

Alternatively, if NTP is not required, disable it entirely by running the following command:

```
ntp disable
```

3.3.15. Sensitive RPC 'rquotad' Service is Enabled (rpc-sensitive-rquotad-svc)*Description:*

The RPC service 'rquotad' (rquota daemon) is a legacy service returning sensitive information (user quotas on filesystems).

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.7:626	Running rquotad service
172.16.1.7:629	Running rquotad service

References:

Source	Reference
CVE	CVE-1999-0625

Vulnerability Solution:

Disable the service entirely or firewall it.

3.3.16. SSH Server Supports 3DES Cipher Suite (ssh-3des-ciphers)*Description:*

Since 3DES (Triple Data Encryption Standard) only provides an effective security of 112 bits, it is considered close to end of life by some agencies. ECRYPT II (from 2012) recommends for generic application independent long-term protection of at least 128 bits security. The same recommendation has also been reported by BSI Germany (from 2015) and ANSSI France (from 2014), 128 bit is the recommended symmetric size and should be mandatory after 2020. While NIST (from 2012) still considers 3DES being appropriate to use until the end of 2030.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:22	Running SSH serviceInsecure 3DES ciphers in use: 3des-cbc
172.16.1.103:22	Running SSH serviceInsecure 3DES ciphers in use: 3des-cbc
172.16.1.111:22	Running SSH serviceInsecure 3DES ciphers in use: 3des-cbc
172.16.1.12:22	Running SSH serviceInsecure 3DES ciphers in use: 3des-cbc
172.16.1.46:22	Running SSH serviceInsecure 3DES ciphers in use: 3des-cbc
172.16.1.7:22	Running SSH serviceInsecure 3DES ciphers in use: 3des-cbc

References:

Source	Reference
URL	http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf
URL	https://bettercrypto.org/static/applied-crypto-hardening.pdf

Vulnerability Solution:

Remove all 3DES ciphers from the cipher list specified in sshd_config.

3.3.17. OpenSSH "X11UseLocalhost" X11 Forwarding Session Hijacking Vulnerability (ssh-openssh-x11uselocalhost-x11-forwarding-session-hijack)*Description:*

OpenSSH before 5.1 sets the SO_REUSEADDR socket option when the X11UseLocalhost configuration setting is disabled, which allows local users on some platforms to hijack the X11 forwarding port via a bind to a single IP address, as demonstrated on the HP-UX platform.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.7:22	OpenBSD OpenSSH 4.3 on Linux 2.6.18

References:

Source	Reference
BID	30339
CVE	CVE-2008-3259
XF	43940

Vulnerability Solution:

OpenBSD OpenSSH < 5.1

Download and apply the upgrade from: <ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH>

While you can always [build OpenSSH from source](#), many platforms and distributions provide pre-built binary packages for OpenSSH. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.3.18. TLS/SSL Server Supports 3DES Cipher Suite (ssl-3des-ciphers)*Description:*

Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) include cipher suites based on the 3DES (Triple Data Encryption Standard) algorithm. Since 3DES only provides an effective security of 112 bits, it is considered close to end of life by some agencies. Consequently, the 3DES algorithm is not included in the specifications for TLS version 1.3. ECRYPT II (from 2012) recommends for generic application independent long-term protection at least 128 bits security. The same recommendation has also been reported by BSI Germany (from 2015) and ANSSI France (from 2014), 128 bit is the recommended symmetric size and should be mandatory after 2020. While NIST (from 2012) still considers 3DES being appropriate to use until the end of 2030.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.1:443	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.1 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.2 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA

Affected Nodes:	Additional Information:
172.16.1.12:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
172.16.1.156:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA
172.16.1.156:3389	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA
172.16.1.180:8181	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.1 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.2 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
172.16.1.25:8181	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
172.16.1.46:5989	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA
172.16.1.7:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS 1.0 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA

References:

Source	Reference
URL	http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295
URL	http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
URL	https://wiki.mozilla.org/Security/Server_Side_TLS
URL	https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Rule_-

Source	Reference
	_Only_Support_Strong_Cryptographic_Ciphers
URL	http://support.microsoft.com/kb/245030/

Vulnerability Solution:

Configure the server to disable support for 3DES suite.

For Microsoft IIS web servers, see Microsoft Knowledgebase article [245030](#) for instructions on disabling 3DES cipher suite.

The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.

Refer to your server vendor documentation to apply the recommended cipher configuration:

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

3.3.19. TLS/SSL Server Does Not Support Any Strong Cipher Algorithms (ssl-only-weak-ciphers)**Description:**

The server is not configured with support for any modern, secure ciphers and only supports ciphers known to be weak against attack.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.12:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_DES_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5 TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA
172.16.1.156:443	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA
172.16.1.46:5989	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA

Affected Nodes:	Additional Information:
	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA
172.16.1.7:443	Negotiated with the following insecure cipher suites: SSL 2.0 ciphers: SSL_CK_DES_192_EDE3_CBC_WITH_MD5 SSL_CK_DES_64_CBC_WITH_MD5 SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5 SSL_CK_RC2_128_CBC_WITH_MD5 SSL_CK_RC4_128_EXPORT40_WITH_MD5 SSL_CK_RC4_128_WITH_MD5

References:

Source	Reference
URL	http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295
URL	https://wiki.mozilla.org/Security/Server_Side_TLS
URL	https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Rule_-_Only_Support_Strong_Cryptographic_Ciphers
URL	http://support.microsoft.com/kb/245030/

Vulnerability Solution:

Enable support for at least one of the ciphers listed below:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

3.3.20. UDP IP ID Zero (udp-ipid-zero)*Description:*

The remote host responded with a UDP packet whose IP ID was zero. Normally the IP ID should be set to a unique value and is used in the reconstruction of fragmented packets. Generally this behavior is only seen with systems derived from a Linux kernel, which may allow an attacker to fingerprint the target's operating system.

Affected Nodes:

Affected Nodes:	Additional Information:
172.16.1.25	Received UDP packet with IP ID of zero:IPv4 SRC[172.16.1.25]

Affected Nodes:	Additional Information:
	<p>TGT[172.16.100.3] TOS[192] TTL[63] Flags[40] Proto[17] ID[0] FragOff[0] HDR-LENGTH[20] TOTAL-LENGTH[76] CKSUM[32164] UDP SRC-PORT[123] TGT-PORT[63299] CKSUM[7070] RAW DATA [48]: 1A040AE80000019400001297BA9B1C93 E369C361DE8CA8B7C6F15EDB78000000 ia^x... E369C3E26B197FCEE369C3E26B1DAE21 ik..ik.!</p>
172.16.1.7	<p>Received UDP packet with IP ID of zero:IPv4 SRC[172.16.1.7] TGT[172.16.100.3] TOS[0] TTL[63] Flags[40] Proto[17] ID[0] FragOff[0] HDR-LENGTH[20] TOTAL-LENGTH[80] CKSUM[32370] UDP SRC-PORT[177] TGT-PORT[63293] CKSUM[10770] RAW DATA [52]: 00010005002E0000000F637265676173cregas 2E637265672E6E657400194C696E7578 .creg.net..Linux 20322E362E31382D3337312E31322E31 2.6.18-371.12.1 2E656C35 .el5</p>

References:

None

Vulnerability Solution:

Many vendors do not consider this to be a vulnerability, or a vulnerability worth fixing, so there are no vendor-provided solutions aside from putting a firewall or other filtering device between the target and hostile attackers that is capable of randomizing IP IDs.

4. Discovered Services

4.1. <unknown>

4.1.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	tcp	657	0	<ul style="list-style-type: none"> •ssl3: false •tlsv1_0: false •tlsv1_1: false •tlsv1_2: false
172.16.1.46	tcp	657	0	<ul style="list-style-type: none"> •ssl3: false •tlsv1_0: false •tlsv1_1: false •tlsv1_2: false
172.16.1.7	tcp	8005	0	<ul style="list-style-type: none"> •ssl3: false •tlsv1_0: false •tlsv1_1: false •tlsv1_2: false

4.2. AIX Web Based Admin

4.2.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	tcp	9090	0	

4.3. CIFS

CIFS, the Common Internet File System, was defined by Microsoft to provide file sharing services over the Internet. CIFS extends the Server Message Block (SMB) protocol designed by IBM and enhanced by Intel and Microsoft. CIFS provides mechanisms for sharing resources (files, printers, etc.) and executing remote procedure calls over named pipes.

4.3.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.156	tcp	139	2	<ul style="list-style-type: none"> •Windows Server 2012 R2 Datacenter 6.3 •domain: CREG •password-mode: encrypt •security-mode: user

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •smb-signing: disabled •smb1-enabled: true
172.16.1.156	tcp	445	2	<ul style="list-style-type: none"> •Windows Server 2012 R2 Datacenter 6.3 •domain: CREG •password-mode: encrypt •security-mode: user •smb-signing: disabled •smb1-enabled: true •smb2-enabled: true •smb2-signing: enabled
172.16.1.25	tcp	139	2	<ul style="list-style-type: none"> •Samba 3.6.23-35.el6_8 •domain: CREG.NET •guest-login: enabled •password-mode: encrypt •security-mode: share •smb-signing: disabled •smb1-enabled: true
172.16.1.25	tcp	445	2	<ul style="list-style-type: none"> •Samba 3.6.23-35.el6_8 •domain: CREG.NET •guest-login: enabled •password-mode: encrypt •security-mode: share •smb-signing: disabled •smb1-enabled: true
172.16.1.7	tcp	139	2	<ul style="list-style-type: none"> •Samba 3.0.33-3.40.el5_10 •domain: IT •guest-login: enabled •password-mode: clear •security-mode: share •smb-signing: disabled •smb1-enabled: true
172.16.1.7	tcp	445	2	<ul style="list-style-type: none"> •Samba 3.0.33-3.40.el5_10 •domain: IT •guest-login: enabled •password-mode: clear •security-mode: share •smb-signing: disabled

Device	Protocol	Port	Vulnerabilities	Additional Information
				•smb1-enabled: true

4.4. CIFS Name Service

CIFS, the Common Internet File System, was defined by Microsoft to provide file sharing services over the Internet. CIFS extends the Server Message Block (SMB) protocol designed by IBM and enhanced by Intel and Microsoft. CIFS provides mechanisms for sharing resources (files, printers, etc.) and executing remote procedure calls over named pipes. This service is used to handle CIFS browsing (name) requests. Responses contain the names and types of services that can be accessed via CIFS named pipes.

4.4.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.156	udp	137	1	<ul style="list-style-type: none"> •advertised-name-1: GESTORNORMATIVO (File Server Service) •advertised-name-2: GESTORNORMATIVO (Computer Name) •advertised-name-3: CREG (Domain Name) •advertised-name-count: 3 •mac-address: 005056A977CF
172.16.1.7	udp	137	1	<ul style="list-style-type: none"> •advertised-name-1: CREGAS (Computer Name) •advertised-name-2: CREGAS (Logged-on User) •advertised-name-3: CREGAS (File Server Service) •advertised-name-4: __MSBROWSE__ (Master Browser) •advertised-name-5: IT (Master Browser) •advertised-name-6: IT (Browser Service Elections) •advertised-name-7: IT (Domain Name) •advertised-name-count: 7 •mac-address: 000000000000

4.5. DCE Endpoint Resolution

The DCE Endpoint Resolution service, aka Endpoint Mapper, is used on Microsoft Windows systems by Remote Procedure Call (RPC) clients to determine the appropriate port number to connect to for a particular RPC service. This is similar to the portmapper service used on Unix systems.

4.5.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.156	tcp	135	0	

4.6. DCE RPC

4.6.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.156	tcp	49152	0	<ul style="list-style-type: none"> •interface-uuid: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D •interface-version: 1 •name: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D •object-interface-uuid: 765294BA-60BC-48B8-92E9-89FD77769D91 •port.discovered.from: tcp/135 •protocol-sequence: ncacn_ip_tcp:172.16.1.156[49152]
172.16.1.156	tcp	49153	0	<ul style="list-style-type: none"> •interface-uuid: 30ADC50C-5CBC-46CE-9A0E-91914789E23C •interface-version: 1 •name: NRP server endpoint •port.discovered.from: tcp/135 •protocol-sequence: ncacn_ip_tcp:172.16.1.156[49153]
172.16.1.156	tcp	49154	0	<ul style="list-style-type: none"> •interface-uuid: 58E604E8-9ADB-4D2E-A464-3B0683FB1480 •interface-version: 1 •name: AppInfo •port.discovered.from: tcp/135 •protocol-sequence: ncacn_ip_tcp:172.16.1.156[49154]
172.16.1.156	tcp	49155	0	<ul style="list-style-type: none"> •interface-uuid: B25A52BF-E5DD-4F4A-AEA6-8CA7272A0E86 •interface-version: 2 •name: KeyIso •port.discovered.from: tcp/135 •protocol-sequence:

Device	Protocol	Port	Vulnerabilities	Additional Information
				ncacn_ip_tcp:172.16.1.156[49155]
172.16.1.156	tcp	49156	0	<ul style="list-style-type: none"> •interface-uuid: 76F03F96-CDFD-44FC-A22C-64950A001209 •interface-version: 1 •name: 76F03F96-CDFD-44FC-A22C-64950A001209 •port.discovered.from: tcp/135 •protocol-sequence: ncacn_ip_tcp:172.16.1.156[49156]
172.16.1.156	tcp	49157	0	<ul style="list-style-type: none"> •interface-uuid: 367ABB81-9844-35F1-AD32-98F038001003 •interface-version: 2 •name: 367ABB81-9844-35F1-AD32-98F038001003 •port.discovered.from: tcp/135 •protocol-sequence: ncacn_ip_tcp:172.16.1.156[49157]
172.16.1.156	tcp	49158	0	<ul style="list-style-type: none"> •interface-uuid: 6B5BDD1E-528C-422C-AF8C-A4079BE4FE48 •interface-version: 1 •name: Remote Fw APIs •port.discovered.from: tcp/135 •protocol-sequence: ncacn_ip_tcp:172.16.1.156[49158]
172.16.1.156	tcp	49159	0	<ul style="list-style-type: none"> •interface-uuid: B25A52BF-E5DD-4F4A-AEA6-8CA7272A0E86 •interface-version: 2 •name: KeyIso •port.discovered.from: tcp/135 •protocol-sequence: ncacn_ip_tcp:172.16.1.156[49159]

4.7. HTTP

HTTP, the HyperText Transfer Protocol, is used to exchange multimedia content on the World Wide Web. The multimedia files commonly used with HTTP include text, sound, images and video.

4.7.1. General Security Issues

Simple authentication scheme

Many HTTP servers use BASIC as their primary mechanism for user authentication. This is a very simple scheme that uses base 64 to encode the cleartext user id and password. If a malicious user is in a position to monitor HTTP traffic, user ids and passwords can be stolen by decoding the base 64 authentication data. To secure the authentication process, use HTTPS (HTTP over TLS/SSL) connections to transmit the authentication data.

4.7.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.1	tcp	80	1	<ul style="list-style-type: none"> •Apache HTTPD •http.banner: Apache •http.banner.server: Apache
172.16.1.12	tcp	80	0	<ul style="list-style-type: none"> •IBM WebSphere •http.banner: Lotus Expeditor Web Container/6.1 •http.banner.server: Lotus Expeditor Web Container/6.1
172.16.1.156	tcp	80	2	<ul style="list-style-type: none"> •Microsoft IIS 8.5 •http.banner: Microsoft-IIS/8.5 •http.banner.server: Microsoft-IIS/8.5 •verbs-1: GET •verbs-2: HEAD •verbs-3: OPTIONS •verbs-4: POST •verbs-5: TRACE •verbs-count: 5
172.16.1.156	tcp	5985	0	<ul style="list-style-type: none"> •Microsoft-HTTPAPI 2.0 •http.banner: Microsoft-HTTPAPI/2.0 •http.banner.server: Microsoft-HTTPAPI/2.0
172.16.1.180	tcp	80	6	<ul style="list-style-type: none"> •Apache HTTPD 2.4.10 •http.banner: Apache/2.4.10 (Debian) •http.banner.server: Apache/2.4.10 (Debian) •verbs-1: GET •verbs-2: HEAD •verbs-3: OPTIONS •verbs-4: POST •verbs-count: 4
172.16.1.180	tcp	4848	0	
172.16.1.180	tcp	8080	2	

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •Oracle GlassFish Server 4.1 •http.banner: GlassFish Server Open Source Edition 4.1 •http.banner.server: GlassFish Server Open Source Edition 4.1 •http.banner.x-powered-by: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition 4.1 Java/Oracle Corporation/1.8) •verbs-1: DELETE •verbs-2: GET •verbs-3: HEAD •verbs-4: OPTIONS •verbs-5: POST •verbs-6: PUT •verbs-7: TRACE •verbs-count: 7
172.16.1.25	tcp	4848	0	<ul style="list-style-type: none"> •Oracle GlassFish Server 3.0.1 •http.banner: GlassFish Server Open Source Edition 3.0.1 •http.banner.server: GlassFish Server Open Source Edition 3.0.1 •http.banner.x-powered-by: JSF/2.0
172.16.1.46	tcp	80	3	<ul style="list-style-type: none"> •Lotus Domino 9.0.0.0 •IBM Lotus Domino •http.banner: Lotus-Domino •http.banner.server: Lotus-Domino
172.16.1.46	tcp	5988	0	
172.16.1.7	tcp	80	3	<ul style="list-style-type: none"> •Apache HTTPD •http.banner: Apache •http.banner.server: Apache •verbs-1: GET •verbs-2: HEAD •verbs-3: OPTIONS •verbs-4: POST •verbs-5: TRACE •verbs-count: 5
172.16.1.7	tcp	631	1	<ul style="list-style-type: none"> •Apple CUPS 1.2

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •http.banner: CUPS/1.2 •http.banner.server: CUPS/1.2 •verbs-1: GET •verbs-2: HEAD •verbs-3: OPTIONS •verbs-4: POST •verbs-5: PUT •verbs-count: 5
172.16.1.7	tcp	7778	3	<ul style="list-style-type: none"> •Apache HTTPD •http.banner: Apache •http.banner.server: Apache •verbs-1: GET •verbs-2: HEAD •verbs-3: OPTIONS •verbs-4: POST •verbs-5: TRACE •verbs-count: 5
172.16.1.7	tcp	8008	2	<ul style="list-style-type: none"> •lighttpd 1.4.35 •http.banner: lighttpd/1.4.35 •http.banner.server: lighttpd/1.4.35 •verbs-1: GET •verbs-2: HEAD •verbs-3: OPTIONS •verbs-4: POST •verbs-count: 4
172.16.1.7	tcp	8080	2	<ul style="list-style-type: none"> •Apache Tomcat •Coyote: 1.1 •http.banner: Apache-Coyote/1.1 •http.banner.server: Apache-Coyote/1.1
172.16.1.7	tcp	8082	2	<ul style="list-style-type: none"> •Apache Tomcat •Coyote: 1.1 •http.banner: Apache-Coyote/1.1 •http.banner.server: Apache-Coyote/1.1
172.16.1.7	tcp	8181	0	

4.8. HTTPS

HTTPS, the HyperText Transfer Protocol over TLS/SSL, is used to exchange multimedia content on the World Wide Web using encrypted (TLS/SSL) connections. Once the TLS/SSL connection is established, the standard HTTP protocol is used. The multimedia files commonly used with HTTP include text, sound, images and video.

4.8.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.1	tcp	443	8	<ul style="list-style-type: none"> •Apache HTTPD •PHP: 7.1.8 •http.banner: Apache •http.banner.server: Apache •http.banner.x-powered-by: PHP/7.1.8 •ssl: true •ssl.cert.issuer.dn: CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US •ssl.cert.key.alg.name: RSA •ssl.cert.key.rsa.modulusBits: 2048 •ssl.cert.not.valid.after: Sat, 13 Nov 2021 07:00:00 COT •ssl.cert.not.valid.before: Wed, 13 Nov 2019 19:00:00 COT •ssl.cert.selfsigned: false •ssl.cert.serial.number: 16887395047672668620674354679802745431 •ssl.cert.sha1.fingerprint: 5fa24ac0ff29f4a9daed66f9322b765961c5ae2e •ssl.cert.sig.alg.name: SHA256withRSA •ssl.cert.subject.alt.name-1: www.creg.gov.co •ssl.cert.subject.alt.name-2: creg.gov.co •ssl.cert.subject.alt.name-count: 2 •ssl.cert.subject.dn: CN=www.creg.gov.co, OU=INFORMATICA Y TECNOLOGIA, O=COMISION DE REGULACION DE ENERGIA Y GAS CREG,

Device	Protocol	Port	Vulnerabilities	Additional Information
				<p>L=BOGOTA, C=CO</p> <ul style="list-style-type: none"> •ssl.cert.validchain: true •ssl.cert.version: 3 •ssl.dh.generator.2048: 2 •ssl.dh.prime.2048: ffffffff90fdaa22168c234c4c6628 b80dc1cd129024e088a67cc74020bbe a63b139b22514a08798e3404ddef951 9b3cd3a431b302b0a6df25f14374fe13 56d6d51c245e485b576625e7ec6f44c 42e9a637ed6b0bff5cb6f406b7edee38 6bfb5a899fa5ae9f24117c4b1fe649286 651ece45b3dc2007cb8a163bf0598da 48361c55d39a69163fa8fd24cf5f83655 d23dca3ad961c62f356208552bb9ed5 29077096966d670c354e4abc9804f17 46c08ca18217c32905e462e36ce3be3 9e772c180e86039b2783a2ec07a28fb 5c55df06f4c52c9de2bcbf6955817183 995497cea956ae515d2261898fa0510 15728e5a8aaca68ffffffffffff •ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2 •sslv2: false •sslv3: false •tlsv1_0: true •tlsv1_0.TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.dh.keysize: 2048 •tlsv1_0.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 2048 •tlsv1_0.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 2048 •tlsv1_0.TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA.dh.keysize: 2048 •tlsv1_0.TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA.dh.keysize: 2048 •tlsv1_0.ciphers: TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AE

Device	Protocol	Port	Vulnerabilities	Additional Information
				<p>S_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_CAMELLIA_256_CBC_SHA</p> <ul style="list-style-type: none"> •tlsv1_0.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS •tlsv1_1: true •tlsv1_1.TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.dh.keysize: 2048 •tlsv1_1.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 2048 •tlsv1_1.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 2048 •tlsv1_1.TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA.dh.keysize: 2048 •tlsv1_1.TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA.dh.keysize: 2048 •tlsv1_1.ciphers: TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_

Device	Protocol	Port	Vulnerabilities	Additional Information
				<p>256_CBC_SHA,TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_CAMELLIA_256_CBC_SHA</p> <p>•tlsv1_1.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS</p> <p>•tlsv1_2: true</p> <p>•tlsv1_2.ciphers: TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_RSA_</p>

Device	Protocol	Port	Vulnerabilities	Additional Information
				<p>WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_GCM_SHA256</p> <p>•tls1_2.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS</p>
172.16.1.12	tcp	443	6	<p>•IBM WebSphere</p> <p>•http.banner: Lotus Expeditor Web Container/6.1</p> <p>•http.banner.server: Lotus Expeditor Web Container/6.1</p> <p>•ssl: true</p> <p>•ssl.cert.chainerror: [Path does not chain with any of the trust anchors]</p> <p>•ssl.cert.issuer.dn: CN=www.ibm.com, OU=STG, O=IBM, L=Austin, ST=TX, C=US</p> <p>•ssl.cert.key.alg.name: RSA</p> <p>•ssl.cert.key.rsa.modulusBits: 1024</p> <p>•ssl.cert.not.valid.after: Mon, 24 Jun 2024 15:51:01 COT</p> <p>•ssl.cert.not.valid.before: Fri, 11 Nov 2005 15:51:01 COT</p> <p>•ssl.cert.selfsigned: true</p> <p>•ssl.cert.serial.number: 1131742261</p> <p>•ssl.cert.sha1.fingerprint: b4435637be15d3b281016aa5ca0b71c ccc9935d6</p> <p>•ssl.cert.sig.alg.name: MD5withRSA</p> <p>•ssl.cert.subject.dn: CN=www.ibm.com, OU=STG, O=IBM, L=Austin, ST=TX, C=US</p> <p>•ssl.cert.validchain: false</p> <p>•ssl.cert.validsignature: true</p> <p>•ssl.cert.version: 3</p> <p>•ssl.dh.generator.1024:</p>

Device	Protocol	Port	Vulnerabilities	Additional Information
				<p>9760508f15230bccb292b982a2eb840bf0581cf5</p> <p>•ssl.dh.generator.512:</p> <p>962eddcc369cba8ebb260ee6b6a126d9346e38c5</p> <p>•ssl.dh.prime.1024:</p> <p>fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbb9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7</p> <p>•ssl.dh.prime.512:</p> <p>fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17</p> <p>•ssl.protocols: sslv3</p> <p>•sslv2: false</p> <p>•sslv3: true</p> <p>•sslv3.TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA.dh.keysize: 512</p> <p>•sslv3.TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.dh.keysize: 1024</p> <p>•sslv3.ciphers:</p> <p>TLS_DHE_RSA_WITH_DES_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_EXPORT_WITH_RC4_40_MD5,TLS_RSA_WITH_RC4_128_MD5,TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5,TLS_RSA_EXPORT_WITH_DES40_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA,TLS_RSA_WITH_DES_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA</p>

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •ssl3.extensions: RENEGOTIATION_INFO •tlsv1_0: false •tlsv1_1: false •tlsv1_2: false
172.16.1.156	tcp	443	5	<ul style="list-style-type: none"> •Microsoft-HTTPAPI 2.0 •http.banner: Microsoft-HTTPAPI/2.0 •http.banner.server: Microsoft-HTTPAPI/2.0 •ssl: true •ssl.cert.issuer.dn: CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB •ssl.cert.key.alg.name: RSA •ssl.cert.key.rsa.modulusBits: 2048 •ssl.cert.not.valid.after: Sat, 24 Apr 2021 18:59:59 COT •ssl.cert.not.valid.before: Thu, 23 Apr 2020 19:00:00 COT •ssl.cert.selfsigned: false •ssl.cert.serial.number: 308329741488551761382818800533 153248587 •ssl.cert.sha1.fingerprint: 141754ca530ab0b0959e141a2137ae8 209899954 •ssl.cert.sig.alg.name: SHA256withRSA •ssl.cert.subject.alt.name-1: *.creg.gov.co •ssl.cert.subject.alt.name-2: creg.gov.co •ssl.cert.subject.alt.name-count: 2 •ssl.cert.subject.dn: CN=*.creg.gov.co •ssl.cert.validchain: true •ssl.cert.version: 3 •ssl.protocols: ssl3,tlsv1_0,tlsv1_1,tlsv1_2

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •ssl3: true •ssl3.ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 •ssl3.extensions: RENEGOTIATION_INFO •tls1_0: true •tls1_0.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 •tls1_0.extensions: RENEGOTIATION_INFO •tls1_1: true •tls1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 •tls1_1.extensions: RENEGOTIATION_INFO •tls1_2: true •tls1_2.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE

Device	Protocol	Port	Vulnerabilities	Additional Information
				_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 •tlsv1_2.extensions: RENEGOTIATION_INFO
172.16.1.180	tcp	8181	6	•Oracle GlassFish Server 4.1 •http.banner: GlassFish Server Open Source Edition 4.1 •http.banner.server: GlassFish Server Open Source Edition 4.1 •http.banner.x-powered-by: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition 4.1 Java/Oracle Corporation/1.8) •ssl: true •ssl.cert.chainerror: [Path does not chain with any of the trust anchors] •ssl.cert.issuer.dn: CN=localhost, OU=GlassFish, O=Oracle Corporation, L=Santa Clara, ST=California, C=US •ssl.cert.key.alg.name: RSA •ssl.cert.key.rsa.modulusBits: 2048 •ssl.cert.not.valid.after: Sun, 18 Aug 2024 08:19:18 COT •ssl.cert.not.valid.before: Thu, 21 Aug 2014 08:19:18 COT •ssl.cert.selfsigned: true •ssl.cert.serial.number: 987539630 •ssl.cert.sha1.fingerprint: b861b9a6558546813c76962c11df716eae2c0fe

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •ssl.cert.sig.alg.name: SHA256withRSA •ssl.cert.subject.dn: CN=localhost, OU=GlassFish, O=Oracle Corporation, L=Santa Clara, ST=California, C=US •ssl.cert.validchain: false •ssl.cert.validsignature: true •ssl.cert.version: 3 •ssl.dh.generator.1024: 2 •ssl.dh.prime.1024: ffffffffffffc90fdaa22168c234c4c6628 b80dc1cd129024e088a67cc74020bbe a63b139b22514a08798e3404ddef951 9b3cd3a431b302b0a6df25f14374fe13 56d6d51c245e485b576625e7ec6f44c 42e9a637ed6b0bff5cb6f406b7edee38 6bfb5a899fa5ae9f24117c4b1fe649286 651ece65381fffffffffffff •ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2 •sslv2: false •sslv3: false •tlsv1_0: true •tlsv1_0.TLS_DHE_RSA_WITH_3DES _EDE_CBC_SHA.dh.keysize: 1024 •tlsv1_0.TLS_DHE_RSA_WITH_AES_ 128_CBC_SHA.dh.keysize: 1024 •tlsv1_0.ciphers: TLS_DHE_RSA_WITH_AES_128_CB C_SHA,TLS_RSA_WITH_AES_128_ CBC_SHA,TLS_ECDHE_RSA_WITH_ AES_128_CBC_SHA,TLS_ECDHE_R SA_WITH_3DES_EDE_CBC_SHA,TL S_RSA_WITH_3DES_EDE_CBC_SH A,TLS_DHE_RSA_WITH_3DES_EDE _CBC_SHA •tlsv1_0.extensions: RENEGOTIATION_INFO •tlsv1_1: true •tlsv1_1.TLS_DHE_RSA_WITH_3DES _EDE_CBC_SHA.dh.keysize: 1024

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •tlsv1_1.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 1024 •tlsv1_1.ciphers: TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA •tlsv1_1.extensions: RENEGOTIATION_INFO •tlsv1_2: true •tlsv1_2.ciphers: TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_GCM_SHA256 •tlsv1_2.extensions: RENEGOTIATION_INFO •verbs-1: DELETE •verbs-2: GET •verbs-3: HEAD •verbs-4: OPTIONS •verbs-5: POST •verbs-6: PUT •verbs-7: TRACE

Device	Protocol	Port	Vulnerabilities	Additional Information
				•verbs-count: 7
172.16.1.25	tcp	8181	6	<ul style="list-style-type: none"> •Oracle GlassFish Server 3.0.1 •http.banner: GlassFish Server Open Source Edition 3.0.1 •http.banner.server: GlassFish Server Open Source Edition 3.0.1 •http.banner.x-powered-by: Servlet/3.0 •ssl: true •ssl.cert.chainerror: [Path does not chain with any of the trust anchors] •ssl.cert.issuer.dn: CN=creg.utp.edu.co, OU=GlassFish, O=Oracle Corporation, L=Santa Clara, ST=California, C=US •ssl.cert.key.alg.name: RSA •ssl.cert.key.rsa.modulusBits: 2048 •ssl.cert.not.valid.after: Mon, 23 Oct 2023 10:15:52 COT •ssl.cert.not.valid.before: Fri, 25 Oct 2013 10:15:52 COT •ssl.cert.selfsigned: true •ssl.cert.serial.number: 854396261 •ssl.cert.sha1.fingerprint: 6b4e65bbdca528edfef4dcb4b0f08c95c374c0c2 •ssl.cert.sig.alg.name: SHA256withRSA •ssl.cert.subject.dn: CN=creg.utp.edu.co, OU=GlassFish, O=Oracle Corporation, L=Santa Clara, ST=California, C=US •ssl.cert.validchain: false •ssl.cert.validsignature: true •ssl.cert.version: 3 •ssl.dh.generator.768: 30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d202

Device	Protocol	Port	Vulnerabilities	Additional Information
				<p>9d83c1c158547f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252</p> <ul style="list-style-type: none"> •ssl.dh.prime.768: e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf •ssl.protocols: tlsv1_0 •sslv2: false •sslv3: false •tlsv1_0: true •tlsv1_0.TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.dh.keysize: 768 •tlsv1_0.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 768 •tlsv1_0.ciphers: TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_ECDHE_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA •tlsv1_0.extensions: RENEGOTIATION_INFO •tlsv1_1: false •tlsv1_2: false •verbs-1: DELETE •verbs-2: GET •verbs-3: HEAD •verbs-4: OPTIONS •verbs-5: POST

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •verbs-6: PUT •verbs-7: TRACE •verbs-count: 7
172.16.1.46	tcp	5989	6	<ul style="list-style-type: none"> •ssl: true •ssl.cert.chainerror: [Path does not chain with any of the trust anchors] •ssl.cert.issuer.dn: CN=PEGASUS TEST CERTIFICATE-DO NOT USE, OU=The OpenPegasus Project, O=The Open Group, L=Reading, ST=Berkshire, C=UK •ssl.cert.key.alg.name: RSA •ssl.cert.key.rsa.modulusBits: 2048 •ssl.cert.not.valid.after: Fri, 27 Mar 2015 02:49:19 COT •ssl.cert.not.valid.before: Tue, 29 Mar 2005 02:49:19 COT •ssl.cert.selfsigned: true •ssl.cert.serial.number: 0 •ssl.cert.sha1.fingerprint: f8942a0e1ee94f55bfd0db14ce583d0a02e72da7 •ssl.cert.sig.alg.name: MD5withRSA •ssl.cert.subject.dn: CN=PEGASUS TEST CERTIFICATE-DO NOT USE, OU=The OpenPegasus Project, O=The Open Group, L=Reading, ST=Berkshire, C=UK •ssl.cert.validchain: false •ssl.cert.validsignature: true •ssl.cert.version: 1 •ssl.protocols: sslv3,tls1_0 •sslv2: false •sslv3: true •sslv3.ciphers: TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5,TLS_RSA_WITH_AES_256_CBC_SHA,TL

Device	Protocol	Port	Vulnerabilities	Additional Information
				<p>S_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_DES_CBC_SHA</p> <ul style="list-style-type: none"> •ssl3.extensions: RENEGOTIATION_INFO •tlsv1_0: true •tlsv1_0.ciphers: TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_DES_CBC_SHA •tlsv1_0.extensions: RENEGOTIATION_INFO •tlsv1_1: false •tlsv1_2: false
172.16.1.7	tcp	443	6	<ul style="list-style-type: none"> •Apache HTTPD •http.banner: Apache •http.banner.server: Apache •ssl: true •ssl.cert.chainerror: [Path does not chain with any of the trust anchors] •ssl.cert.issuer.dn: CN=Certificado Empresarial Clase-A, O=Certicamara S.A. Entidad de Certificacion, L=Carrera 9 16-21 Bogota, C=CO •ssl.cert.key.alg.name: RSA •ssl.cert.key.rsa.modulusBits: 1024 •ssl.cert.not.valid.after: Wed, 14 Nov 2007 16:51:08 COT •ssl.cert.not.valid.before: Tue, 14 Nov 2006 16:51:08 COT •ssl.cert.selfsigned: false •ssl.cert.serial.number: 150967983768992043628194610465822429980 •ssl.cert.sha1.fingerprint: b35a9e8f3d205c991e95f6b9dd393a73af7b399c

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •ssl.cert.sig.alg.name: SHA1withRSA •ssl.cert.subject.dn: EMAILADDRESS=soporte@creg.gov.co, CN=cregas.creg.gov.co, OU=SISTEMAS E INFORMACION, O=COMISION DE REGULACION DE ENERGIA Y GAS - CREG, L=BOGOTA, ST=D.C., C=CO •ssl.cert.validchain: false •ssl.cert.version: 3 •ssl.dh.generator.1024: 2 •ssl.dh.generator.512: 2 •ssl.dh.prime.1024: e6969d3d495be32c7cf180c3bdd4798 e91b7818251bb055e2a2064904a79a 770fa15a259cbd523a6a6ef09c43048d 5a22f971f3c20129b48000e6edd061cb c053e371d794e5327df611ebbbe1bac 9b5c6044cf023d76e05eea9bad991b1 3a63c974e9ef1839eb5db125136f7262 e56a8871538dfd823c6505085e21f0dd 5c86b •ssl.dh.prime.512: d4bcd52406f69b35994b88de5db8968 2c8157f62d8f33633ee5772f11f05ab22 d6b5145b9f241e5acc31ff090a4bc711 48976f76795094e71e7903529f5a824 b •ssl.protocols: sslv3,tls1_0 •sslv2: true •sslv2.ciphers: SSL CK RC4 128 WITH MD5,SSL CK RC4 128 EXPORT40 WITH MD5,SSL CK RC2 128 CBC WITH MD5,SSL CK RC2 128 CBC EXPORT40 WITH MD5,SSL CK DES 64 CBC WITH MD5,SSL CK DES 192 EDE3 CBC WITH MD5 •sslv3: true •sslv3.TLS_DHE_RSA_EXPORT_WIT

Device	Protocol	Port	Vulnerabilities	Additional Information
				<p>H_DES40_CBC_SHA.dh.keysize: 512</p> <ul style="list-style-type: none"> •ssl3.TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.dh.keysize: 1024 •ssl3.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 1024 •ssl3.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 1024 •ssl3.ciphers: <p>TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_DES_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_EXPORT_WITH_RC4_40_MD5,TLS_RSA_WITH_RC4_128_MD5,TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_EXPORT_WITH_DES40_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA,TLS_RSA_WITH_DES_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA</p> •ssl3.extensions: <p>RENEGOTIATION_INFO</p> •tlsv1_0: true •tlsv1_0.TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA.dh.keysize: 512 •tlsv1_0.TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.dh.keysize: 1024 •tlsv1_0.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 1024 •tlsv1_0.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 1024 •tlsv1_0.ciphers: <p>TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_DES_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA</p>

Device	Protocol	Port	Vulnerabilities	Additional Information
				<p>S_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_EXPORT_WITH_RC4_40_MD5,TLS_RSA_WITH_RC4_128_MD5,TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_EXPORT_WITH_DES40_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA,TLS_RSA_WITH_DES_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA</p> <ul style="list-style-type: none"> •tls1_0.extensions: RENEGOTIATION_INFO •tls1_1: false •tls1_2: false •verbs-1: GET •verbs-2: HEAD •verbs-3: OPTIONS •verbs-4: POST •verbs-5: TRACE •verbs-count: 5
181.118.158.2	tcp	8443	3	<ul style="list-style-type: none"> •xxxxxxxx-xxxxx •http.banner: xxxxxxxx-xxxxx •http.banner.server: xxxxxxxx-xxxxx •ssl: true •ssl.cert.chainerror: [Path does not chain with any of the trust anchors] •ssl.cert.issuer.dn: EMAILADDRESS=support@fortinet.com, CN=fortinet-subca2001, OU=Certificate Authority, O=Fortinet, L=Sunnyvale, ST=California, C=US •ssl.cert.key.alg.name: RSA •ssl.cert.key.rsa.modulusBits: 2048 •ssl.cert.not.valid.after: Tue, 18 Jan 2056 22:14:07 COT •ssl.cert.not.valid.before: Fri, 01 Jun

Device	Protocol	Port	Vulnerabilities	Additional Information
				<p>2018 11:00:30 COT</p> <ul style="list-style-type: none"> •ssl.cert.selfsigned: false •ssl.cert.serial.number: 133659 •ssl.cert.sha1.fingerprint: f2f50f772acb3d298ea2a4ba1a4429a5b8623cf4 •ssl.cert.sig.alg.name: SHA256withRSA •ssl.cert.subject.dn: EMAILADDRESS=support@fortinet.com, CN=FG3H1ETB18901831, OU=FortiGate, O=Fortinet, L=Sunnyvale, ST=California, C=US •ssl.cert.validchain: false •ssl.cert.version: 3 •ssl.dh.generator.2048: 2 •ssl.dh.prime.2048: ffffffffffffc90fdaa22168c234c4c6628b80dc1cd129024e088a67cc74020bbea63b139b22514a08798e3404ddef9519b3cd3a431b302b0a6df25f14374fe1356d6d51c245e485b576625e7ec6f44c42e9a637ed6b0bff5cb6f406b7edee386bfb5a899fa5ae9f24117c4b1fe649286651ece45b3dc2007cb8a163bf0598da48361c55d39a69163fa8fd24cf5f83655d23dca3ad961c62f356208552bb9ed529077096966d670c354e4abc9804f1746c08ca18217c32905e462e36ce3be39e772c180e86039b2783a2ec07a28fb5c55df06f4c52c9de2bcbf6955817183995497cea956ae515d2261898fa051015728e5a8aaca68ffffffffffff •ssl.protocols: tlsv1_1,tlsv1_2 •sslv2: false •sslv3: false •tlsv1_0: false •tlsv1_1: true •tlsv1_1.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 2048

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •tlsv1_1.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 2048 •tlsv1_1.TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA.dh.keysize: 2048 •tlsv1_1.TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA.dh.keysize: 2048 •tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_128_CBC_SHA •tlsv1_1.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS •tlsv1_2: true •tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_256_CCM_8,TLS_DHE_RSA_WITH_AES_256_CCM,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384,TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_C

Device	Protocol	Port	Vulnerabilities	Additional Information
				<p>BC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_CCM_8,TLS_RSA_WITH_AES_256_CCM,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_128_CCM_8,TLS_DHE_RSA_WITH_AES_128_CCM,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256,TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CCM_8,TLS_RSA_WITH_AES_128_CCM,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_128_CBC_SHA</p> <p>•tlsv1_2.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS</p> <p>•verbs-1: GET</p> <p>•verbs-2: HEAD</p> <p>•verbs-3: OPTIONS</p> <p>•verbs-count: 3</p>

4.9. Lotus Notes

Lotus Notes/Domino is a groupware system providing users with e-mail, calendaring, scheduling, etc. When using the native Lotus Notes/Domino protocol to access servers, certificate based authentication is performed by default. Combining this with Access Control Lists (ACLs), organizations can permit only trusted users to access servers. The protocol also allows for encryption of data between the client and server.

4.9.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.46	tcp	1352	1	<ul style="list-style-type: none"> •port-encryption-required: no •server-name: CN=Zeus/O=CREG

4.10. MySQL

4.10.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.111	tcp	3306	1	<ul style="list-style-type: none"> •MariaDB 5.5.65 •logging: disabled •protocolVersion: 10 •service.banner: 5.5.65-MariaDB

4.11. NFS

The Network File System provides remote file access to shared file systems across a network. NFS provides methods to list and browse directories and to access and alter files. NFS is built on the RPC protocol and is thus independent of machine, operating systems, or even underlying protocol. The main NFS protocol often operates in tandem with other NFS style protocols. The NFS Mount protocol deals with attaching the remote file systems to a point on the local machine's file system, and advertising what file systems are available to be mounted. The NFS Lock manager adds support for file locking to prevent the occurrence of file change conflicts.

4.11.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.7	udp	2049	0	<ul style="list-style-type: none"> •port.discovered.from: tcp/111 •program-number: 100003 •program-version: 4
172.16.1.7	tcp	2049	0	<ul style="list-style-type: none"> •port.discovered.from: tcp/111 •program-number: 100003 •program-version: 4

4.12. NFS lockd

The Network File System provides remote file access to shared file systems across a network. NFS provides methods to list and browse directories and to access and alter files. NFS is built on the RPC protocol and is thus independent of machine, operating systems, or even underlying protocol. This service, NFS Lock manager, adds support for file locking to prevent the occurrence of file change conflicts. Since the NFS protocol is stateless, the NFS Lock Manager takes care of all the stateful aspects of file locking across

a network

4.12.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	udp	32780	0	<ul style="list-style-type: none"> •port.discovered.from: tcp/111 •program-number: 100021 •program-version: 4
172.16.1.12	tcp	49400	0	<ul style="list-style-type: none"> •port.discovered.from: udp/111 •program-number: 100021 •program-version: 4
172.16.1.7	udp	32769	0	<ul style="list-style-type: none"> •port.discovered.from: udp/111 •program-number: 100021 •program-version: 4
172.16.1.7	tcp	32803	0	<ul style="list-style-type: none"> •port.discovered.from: udp/111 •program-number: 100021 •program-version: 4

4.13. NTP

The Network Time Protocol (NTP) is used to keep the clocks of machines on a network synchronized. Provisions are made in the protocol to account for network disruption and packet latency.

4.13.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	udp	123	2	<ul style="list-style-type: none"> •IBM NTP •ntp.variables: system="UNIX/AIX", leap=0, stratum=4, rootdelay=5.58, rootdispersion=62.03, peer=56078, refid=186.155.28.147, reftime=0xe369c146.635a0000, poll=6, clock=0xe369c162.a822f000, phase=-0.043, freq=3404.53, error=0.03
172.16.1.156	udp	123	0	
172.16.1.25	udp	123	0	
172.16.1.7	udp	123	0	

4.14. Oracle TNS Listener

4.14.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	tcp	1521	1	•Oracle Database 11.2.0.4

4.15. POP

The Post Office Protocol allows workstations to retrieve e-mail dynamically from a mailbox server.

4.15.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.46	tcp	110	1	•pop.banner: +OK IBM Notes POP3 server version Release 9.0.1FP4 ready on Zeus/CREG. •pop.plaintext.authentication: true

4.16. POPS

The Post Office Protocol allows workstations to retrieve e-mail dynamically from a mailbox server. POPS simply adds SSL support to POP3.

4.16.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.46	tcp	995	0	•ssl3: false •tlsv1_0: false •tlsv1_1: false •tlsv1_2: false

4.17. PyramidSys5

4.17.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	udp	32801	0	•port.discovered.from: tcp/111 •program-number: 200001 •program-version: 1
172.16.1.12	udp	32808	0	•port.discovered.from: udp/111 •program-number: 200001 •program-version: 2
172.16.1.12	tcp	33262	0	•port.discovered.from: tcp/111 •program-number: 200001 •program-version: 2

4.18. RDP

4.18.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.156	tcp	3389	4	<ul style="list-style-type: none"> •Microsoft Terminal Service •ssl: true •ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2 •sslv3: false •tlsv1_0: true •tlsv1_0.ciphers: TLS_ECDHE_RSA_WITH_AES_256_ CBC_SHA,TLS_ECDHE_RSA_WITH_ AES_128_CBC_SHA,TLS_RSA_WIT H_AES_256_CBC_SHA,TLS_RSA_W ITH_AES_128_CBC_SHA,TLS_RSA_ WITH_3DES_EDE_CBC_SHA,TLS_R SA_WITH_RC4_128_SHA,TLS_RSA_ WITH_RC4_128_MD5 •tlsv1_0.extensions: RENEGOTIATION_INFO •tlsv1_1: true •tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_ CBC_SHA,TLS_ECDHE_RSA_WITH_ AES_128_CBC_SHA,TLS_RSA_WIT H_AES_256_CBC_SHA,TLS_RSA_W ITH_AES_128_CBC_SHA,TLS_RSA_ WITH_3DES_EDE_CBC_SHA,TLS_R SA_WITH_RC4_128_SHA,TLS_RSA_ WITH_RC4_128_MD5 •tlsv1_1.extensions: RENEGOTIATION_INFO •tlsv1_2: true •tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_AES_256_ CBC_SHA384,TLS_ECDHE_RSA_WI TH_AES_128_CBC_SHA256,TLS_EC DHE_RSA_WITH_AES_256_CBC_S HA,TLS_ECDHE_RSA_WITH_AES_1 28_CBC_SHA,TLS_DHE_RSA_WITH

Device	Protocol	Port	Vulnerabilities	Additional Information
				_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 •tls1_2.extensions: RENEGOTIATION_INFO
172.16.1.180	tcp	3389	0	•xrdp •ssl: false •sslv2: false •sslv3: false •tls1_0: false •tls1_1: false •tls1_2: false

4.19. RPC

4.19.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	udp	2049	0	•port.discovered.from: udp/111 •program-number: 200006 •program-version: 4
172.16.1.12	tcp	2049	0	•port.discovered.from: tcp/111 •program-number: 200006 •program-version: 4
172.16.1.12	udp	32778	0	•port.discovered.from: tcp/111 •program-number: 400005 •program-version: 1

4.20. Remote Execution

Remote Execution, rexec, is used to execute a command on a remote system.

4.20.1. General Security Issues

Authentication easily spoofed

The Remote Execution protocol does not use userid/password authentication to validate users. Instead it uses trust relationships based on information that is easily spoofed by an attacker. When a client connects to a rexec server, it sends a user name to the server. The server verifies client access by: 1. verifying the client's TCP port is reserved (below 1024) 2. verifying that the specified user name exists 3. verifying the client's IP address is in /etc/hosts.equiv file (or /.rhosts if root was specified as the user name). 4. verifying that logins have not been disabled (eg, /etc/nologin).

4.20.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	tcp	512	1	<ul style="list-style-type: none"> •sslv3: false •tlsv1_0: false •tlsv1_1: false •tlsv1_2: false

4.21. Remote Shell

Remote Shell, rsh, is used to open a shell on the remote system. Once a shell is established, the client can execute commands on the remote system and receive the program output.

4.21.1. General Security Issues

Authentication easily spoofed

The Remote Shell protocol does not use userid/password authentication to validate users. Instead it uses trust relationships based on information that is easily spoofed by an attacker. When a client connects to a rsh server, it sends a user name to the server. The server verifies client access by: 1. verifying the client's TCP port is reserved (below 1024) 2. verifying that the specified user name exists 3. verifying the client's IP address is in /etc/hosts.equiv file (or /.rhosts if root was specified as the user name). 4. verifying that logins have not been disabled (eg, /etc/nologin).

4.21.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	tcp	514	1	

4.22. SMTP

SMTP, the Simple Mail Transfer Protocol, is the Internet standard way to send e-mail messages between hosts. Clients typically submit outgoing e-mail to their SMTP server, which then forwards the message on through other SMTP servers until it reaches its final destination.

4.22.1. General Security Issues

Installed by default

By default, most UNIX workstations come installed with the sendmail (or equivalent) SMTP server to handle mail for the local host (e.g. the output of some cron jobs is sent to the root account via email). Check your workstations to see if sendmail is running, by telnetting to port 25/tcp. If sendmail is running, you will see something like this: \$ telnet mybox 25 Trying 192.168.0.1... Connected to mybox.

Escape character is '^]'. 220 mybox. ESMTP Sendmail 8.12.2/8.12.2; Thu, 9 May 2002 03:16:26 -0700 (PDT) If sendmail is running and you don't need it, then disable it via /etc/rc.conf or your operating system's equivalent startup configuration file. If you do need SMTP for the localhost, make sure that the server is only listening on the loopback interface (127.0.0.1) and is not reachable by other hosts. Also be sure to check port 587/tcp, which some versions of sendmail use for outgoing mail submissions.

Promiscuous relay

Perhaps the most common security issue with SMTP servers is servers which act as a "promiscuous relay", or "open relay". This describes servers which accept and relay mail from anywhere to anywhere. This setup allows unauthenticated 3rd parties (spammers) to use your mail server to send their spam to unwitting recipients. Promiscuous relay checks are performed on all discovered SMTP servers. See "smtp-general-openrelay" for more information on this vulnerability and how to fix it.

4.22.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.46	tcp	25	1	<ul style="list-style-type: none"> •Lotus Domino •advertise-esmtp: 1 •advertised-esmtp-extension-count: 4 •advertises-esmtp: true •smtp.banner: 220 ESMTP Service ready at Thu, 26 Nov 2020 00:54:00 - 0500 •smtp.plaintext.authentication: true •supported-auth-method-count: 1 •supported-auth-method:1: LOGIN •supports-auth: true •supports-debug: FALSE •supports-expand: FALSE •supports-help: true •supports-pipelining: true •supports-size: true •supports-turn: FALSE •supports-verify: FALSE
181.118.158.2	tcp	25	0	<ul style="list-style-type: none"> •ssl3: false •tls1_0: false •tls1_1: false •tls1_2: false

4.23. SNMP

Simple Network Management Protocol (SNMP), like the name implies, is a simple protocol used to manage networking appliances by remote clients. It is primarily UDP-based and uses trivial authentication by means of a secret community name.

4.23.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	udp	161	2	<ul style="list-style-type: none"> •assignedNumber: 2 •snmp.banner: IBM PowerPC CHRP Computer.Machine Type: 0x0800004c Processor id: 0008A35AD400.Base Operating System Runtime AIX version: 06.01.0006.0000.TCP/IP Client Support version: 06.01.0006.0001 •snmp.name: cregbd •snmp.sysObjectID: 1.3.6.1.4.1.2.3.1.2.1.1.3 •snmp.uptime: 320 days, 9:00:01.00 •sysDescr: IBM PowerPC CHRP Computer Machine Type: 0x0800004c Processor id: 0008A35AD400 Base Operating System Runtime AIX version: 06.01.0006.0000 TCP/IP Client Support version: 06.01.0006.0001
172.16.1.46	udp	161	0	

4.24. SSH

SSH, or Secure SHell, is designed to be a replacement for the aging Telnet protocol. It primarily adds encryption and data integrity to Telnet, but can also provide superior authentication mechanisms such as public key authentication.

4.24.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.1	tcp	22	4	<ul style="list-style-type: none"> •OpenBSD OpenSSH 7.4 •ssh.algorithms.compression: none,zlib@openssh.com •ssh.algorithms.encryption: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc •ssh.algorithms.hostkey: ssh-rsa,rsa-

Device	Protocol	Port	Vulnerabilities	Additional Information
				sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519 •ssh.algorithms.kex: curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1 •ssh.algorithms.mac: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 •ssh.banner: SSH-2.0-OpenSSH_7.4 •ssh.protocol.version: 2.0 •ssh.rsa.pubkey.fingerprint: 4E7505914C40395F68C7147308064 CBA
172.16.1.103	tcp	22	4	•OpenBSD OpenSSH 7.4 •ssh.algorithms.compression: none,zlib@openssh.com •ssh.algorithms.encryption: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc •ssh.algorithms.hostkey: ssh-rsa,rsa-

Device	Protocol	Port	Vulnerabilities	Additional Information
				sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519 •ssh.algorithms.kex: curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1 •ssh.algorithms.mac: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 •ssh.banner: SSH-2.0-OpenSSH_7.4 •ssh.protocol.version: 2.0 •ssh.rsa.pubkey.fingerprint: 7F323AE335F421632FDE7A6EC89E85BF
172.16.1.111	tcp	22	4	•OpenBSD OpenSSH 7.4 •ssh.algorithms.compression: none,zlib@openssh.com •ssh.algorithms.encryption: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc •ssh.algorithms.hostkey: ssh-rsa,rsa-

Device	Protocol	Port	Vulnerabilities	Additional Information
				sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519 •ssh.algorithms.kex: curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1 •ssh.algorithms.mac: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 •ssh.banner: SSH-2.0-OpenSSH_7.4 •ssh.protocol.version: 2.0 •ssh.rsa.pubkey.fingerprint: 3376A218C0543280BCAF923E5C9E4A57
172.16.1.12	tcp	22	4	•OpenBSD OpenSSH 5.4 •ssh.algorithms.compression: none,zlib@openssh.com •ssh.algorithms.encryption: aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se •ssh.algorithms.hostkey: ssh-rsa,ssh-dss

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •ssh.algorithms.kex: diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1 •ssh.algorithms.mac: hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96 •ssh.banner: SSH-2.0-OpenSSH_5.4 •ssh.protocol.version: 2.0 •ssh.rsa.pubkey.fingerprint: 54E4D98CD77AF86AB6A0B7E96C17ECB7
172.16.1.180	tcp	22	1	<ul style="list-style-type: none"> •OpenBSD OpenSSH 6.7p1 •ssh.algorithms.compression: none,zlib@openssh.com •ssh.algorithms.encryption: aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com •ssh.algorithms.hostkey: ssh-rsa,ssh-dss,ecdsa-sha2-nistp256,ssh-ed25519 •ssh.algorithms.kex: diffie-hellman-group1-sha1 •ssh.algorithms.mac: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 •ssh.banner: SSH-2.0-OpenSSH_6.7p1 Debian-5 •ssh.protocol.version: 2.0

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •ssh.rsa.pubkey.fingerprint: 8CF1F90A4DE70CD7C56D061B6F6B8A1F
172.16.1.25	tcp	4000	0	<ul style="list-style-type: none"> •OpenBSD OpenSSH 5.3 •ssh.banner: SSH-2.0-OpenSSH_5.3 •ssh.protocol.version: 2.0 •ssh.rsa.pubkey.fingerprint: 0C5E8B05228C88D3AC3D3CD1D8105885
172.16.1.46	tcp	22	4	<ul style="list-style-type: none"> •OpenBSD OpenSSH 5.8 •ssh.algorithms.compression: none,zlib@openssh.com •ssh.algorithms.encryption: aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se •ssh.algorithms.hostkey: ssh-rsa,ssh-dss •ssh.algorithms.kex: diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1 •ssh.algorithms.mac: hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96 •ssh.banner: SSH-2.0-OpenSSH_5.8 •ssh.protocol.version: 2.0 •ssh.rsa.pubkey.fingerprint: D4BF89E1DEEDC895BE278DFF63333308
172.16.1.7	tcp	22	5	<ul style="list-style-type: none"> •OpenBSD OpenSSH 4.3 •ssh.algorithms.compression: none,zlib@openssh.com •ssh.algorithms.encryption: aes128-

Device	Protocol	Port	Vulnerabilities	Additional Information
				ctr,aes192-ctr,aes256- ctr,arcfour256,arcfour128,aes128- cbc,3des-cbc,blowfish-cbc,cast128- cbc,aes192-cbc,aes256- cbc,arcfour,rijndael-cbc@lysator.liu.se •ssh.algorithms.hostkey: ssh-rsa,ssh- dss •ssh.algorithms.kex: diffie-hellman- group-exchange-sha1,diffie-hellman- group14-sha1,diffie-hellman-group1- sha1 •ssh.algorithms.mac: hmac-md5,hmac- sha1,hmac-ripemd160,hmac- ripemd160@openssh.com,hmac- sha1-96,hmac-md5-96 •ssh.banner: SSH-2.0-OpenSSH_4.3 •ssh.protocol.version: 2.0 •ssh.rsa.pubkey.fingerprint: D3EDD2EF2116903C8816D3DF7D7F D08A

4.25. Service Location

4.25.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.46	tcp	427	0	

4.26. XWindows

4.26.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.7	tcp	6000	1	

4.27. cmsd

4.27.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	udp	32812	0	•port.discovered.from: udp/111

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •program-number: 100068 •program-version: 5

4.28. daytime

A server providing the daytime service returns the current date and time (as a character string) back to the querying host, regardless of input. The format of the date/time string is unspecified. Its primary use is for debugging and measurement.

4.28.1. General Security Issues

Diagnostics Denial-of-Service Attacks

Many implementations of diagnostics services (like echo, chargen, daytime, and discard) are vulnerable to denial-of-service attacks which flood the service with diagnostics requests, causing the device to spend all its CPU power processing these requests (instead of doing what it should be doing). One common attack against the echo service involves spoofing echo requests so that the device sends echo replies back its own echo service, causing an infinite loop which uses up bandwidth and CPU. This can also be achieved by tricking the chargen service to spam bytes at the echo service, and so on. For more information on the Echo UDP Looping vulnerability, see the paper by Peter Shipley entitled "TCP/IP Weaknesses and Vulnerabilities": <http://www.dis.org/filez/vun-1s.pdf> Many Cisco devices come with these diagnostics services enabled by default. For more information on how Cisco to protect Cisco devices from diagnostics DoS attacks, see the following white paper: <http://www.cisco.com/warp/public/707/3.html> Diagnostics services should always be blocked at the firewall. In addition, if you don't use the diagnostic services, you should disable them.

4.28.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	udp	13	0	
172.16.1.12	tcp	13	0	

4.29. dtspcd

4.29.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	tcp	6112	0	<ul style="list-style-type: none"> •ssl3: false •tlsv1_0: false •tlsv1_1: false •tlsv1_2: false

4.30. fics (Free Internet Chess Server)

4.30.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.7	tcp	5000	0	

4.31. mDNS

4.31.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.180	udp	5353	0	<ul style="list-style-type: none"> •dns-sd-1: _http._tcp.local. •dns-sd-2: _workstation._tcp.local. •dns-sd-count: 2 •mac-address: 00:50:56:8c:21:84

4.32. memcached

4.32.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.1	udp	11211	0	•Memcached 1.4.15
172.16.1.1	tcp	11211	0	•Memcached 1.4.15
172.16.1.1	udp	11211	1	

4.33. mountd

4.33.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	udp	32777	0	<ul style="list-style-type: none"> •port.discovered.from: tcp/111 •program-number: 100005 •program-version: 3
172.16.1.12	tcp	65086	0	<ul style="list-style-type: none"> •port.discovered.from: tcp/111 •program-number: 100005 •program-version: 3
172.16.1.7	tcp	892	0	<ul style="list-style-type: none"> •port.discovered.from: udp/111 •program-number: 100005 •program-version: 3
172.16.1.7	udp	892	0	<ul style="list-style-type: none"> •port.discovered.from: udp/111 •program-number: 100005 •program-version: 3

4.34. nsm_addrand

4.34.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	udp	32794	0	<ul style="list-style-type: none"> •port.discovered.from: udp/111 •program-number: 100133 •program-version: 1

4.35. portmapper

The Remote Procedure Call portmapper is a service that maps RPC programs to specific ports, and provides that information to client programs. Since most RPC programs do not have a well defined port number, they are dynamically allocated a port number when they are first run. Any client program that wishes to use a particular RPC program first contacts the portmapper to determine the port and protocol of the specified RPC program. The client then uses that information to contact the RPC program directly. In addition some implementations of the portmapper allow tunneling commands to RPC programs through the portmapper.

4.35.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.103	udp	111	0	<ul style="list-style-type: none"> •port.discovered.from: tcp/111 •program-number: 100000 •program-version: 2
172.16.1.103	tcp	111	0	<ul style="list-style-type: none"> •port.discovered.from: tcp/111 •program-number: 100000 •program-version: 2
172.16.1.111	udp	111	0	<ul style="list-style-type: none"> •port.discovered.from: tcp/111 •program-number: 100000 •program-version: 2
172.16.1.111	tcp	111	0	<ul style="list-style-type: none"> •port.discovered.from: tcp/111 •program-number: 100000 •program-version: 2
172.16.1.12	udp	111	0	<ul style="list-style-type: none"> •port.discovered.from: udp/111 •program-number: 100000 •program-version: 2
172.16.1.12	tcp	111	0	<ul style="list-style-type: none"> •port.discovered.from: udp/111 •program-number: 100000 •program-version: 2
172.16.1.180	udp	111	0	<ul style="list-style-type: none"> •port.discovered.from: udp/111 •program-number: 100000 •program-version: 2
172.16.1.180	tcp	111	0	<ul style="list-style-type: none"> •port.discovered.from: udp/111

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •program-number: 100000 •program-version: 2
172.16.1.25	udp	111	0	<ul style="list-style-type: none"> •port.discovered.from: tcp/111 •program-number: 100000 •program-version: 2
172.16.1.25	tcp	111	0	<ul style="list-style-type: none"> •port.discovered.from: tcp/111 •program-number: 100000 •program-version: 2
172.16.1.7	udp	111	0	<ul style="list-style-type: none"> •port.discovered.from: udp/111 •program-number: 100000 •program-version: 2
172.16.1.7	tcp	111	0	<ul style="list-style-type: none"> •port.discovered.from: udp/111 •program-number: 100000 •program-version: 2

4.36. rquotad

4.36.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.7	udp	626	1	<ul style="list-style-type: none"> •port.discovered.from: udp/111 •program-number: 100011 •program-version: 2
172.16.1.7	tcp	629	1	<ul style="list-style-type: none"> •port.discovered.from: tcp/111 •program-number: 100011 •program-version: 2

4.37. smux (SNMP Unix Multiplexer)

4.37.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	tcp	199	0	<ul style="list-style-type: none"> •ssl3: false •tls1_0: false •tls1_1: false •tls1_2: false
172.16.1.46	tcp	199	0	<ul style="list-style-type: none"> •ssl3: false •tls1_0: false

Device	Protocol	Port	Vulnerabilities	Additional Information
				<ul style="list-style-type: none"> •tlsv1_1: false •tlsv1_2: false

4.38. status

4.38.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	udp	32787	0	<ul style="list-style-type: none"> •port.discovered.from: udp/111 •program-number: 100024 •program-version: 1
172.16.1.25	udp	22746	0	<ul style="list-style-type: none"> •port.discovered.from: udp/111 •program-number: 100024 •program-version: 1
172.16.1.25	tcp	56206	0	<ul style="list-style-type: none"> •port.discovered.from: tcp/111 •program-number: 100024 •program-version: 1
172.16.1.7	udp	662	0	<ul style="list-style-type: none"> •port.discovered.from: tcp/111 •program-number: 100024 •program-version: 1
172.16.1.7	tcp	662	0	<ul style="list-style-type: none"> •port.discovered.from: tcp/111 •program-number: 100024 •program-version: 1

4.39. timeserver

This service provides a standard, machine-readable date and time. A queried server will return its current time in seconds since midnight on January 1, 1900. This service can be used to correct or verify the time on a particular host and it can be used to synchronize clocks across a network.

4.39.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	tcp	37	0	•server-time: 18841019T182522000
172.16.1.12	udp	37	0	•server-time: 18841019T182522000

4.40. ttdbserverd

4.40.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
--------	----------	------	-----------------	------------------------

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.12	tcp	58991	0	<ul style="list-style-type: none">•port.discovered.from: udp/111•program-number: 100083•program-version: 1

4.41. xdmcp

4.41.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.1.46	udp	177	0	
172.16.1.7	udp	177	0	

5. Discovered Users and Groups

No user or group information was discovered during the scan.

6. Discovered Databases

6.1. HTTP

6.1.1. 172.16.1.46

- /AgentRunner.nsf
- /admin4.nsf
- /catalog.nsf
- /certlog.nsf
- /certsrv.nsf
- /cldbdir.nsf
- /dbdirman.nsf
- /doladmin.nsf
- /domcfg.nsf
- /events4.nsf
- /help/decsdoc.nsf
- /help/lccon.nsf
- /help/lxslc.nsf
- /log.nsf
- /mail.box
- /mail1.box
- /mail2.box
- /mtdata/mtstore.nsf
- /names.nsf
- /reports.nsf
- /statrep.nsf
- /webadmin.nsf

7. Discovered Files and Directories

No file or directory information was discovered during the scan.

8. Policy Evaluations

No policy evaluations were performed.

9. Spidered Web Sites

No web sites were spidered during the scan.