



HIPAA Assessment

External Vulnerability Scan Detail Report



CONFIDENTIALITY NOTE: The information contained in this report is for the exclusive use of the client specified above and may contain confidential, privileged, and non-disclosable information. If you are not the client or addressee, you are strictly prohibited from reading, photocopying, distributing, or otherwise using this report or its contents in any way.

Scan Date: 13-Feb-2020

Prepared for:
HIPAA – Covered Entity
Prepared by:
AMS Networks

13-Feb-2020

Table of Contents

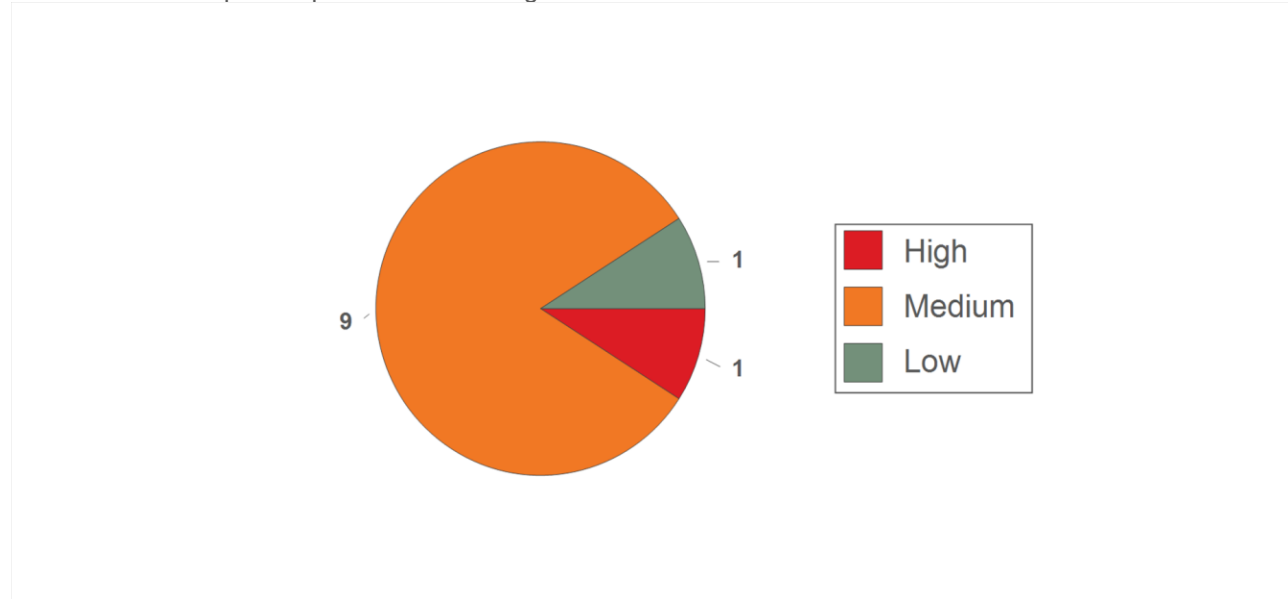
1 - [Summary](#)

2 - [Details](#)

2.1 - [208.32.211.104](#)

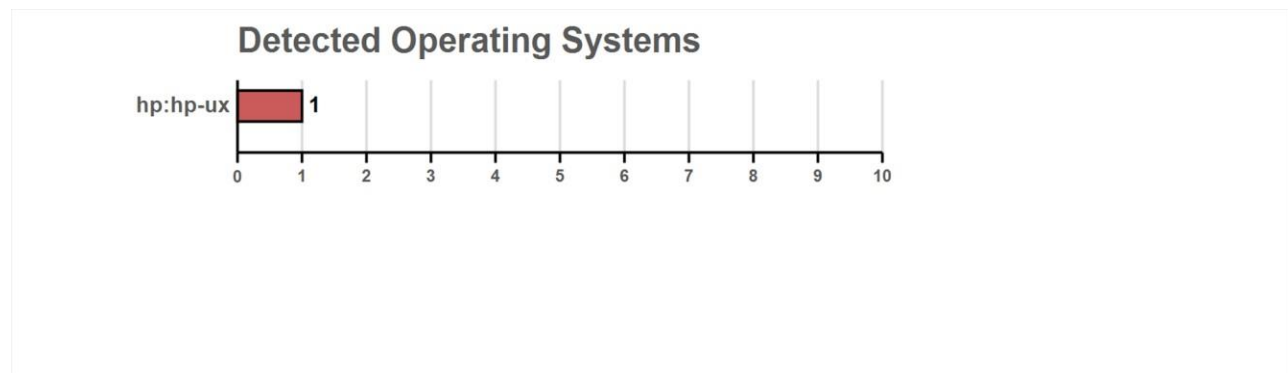
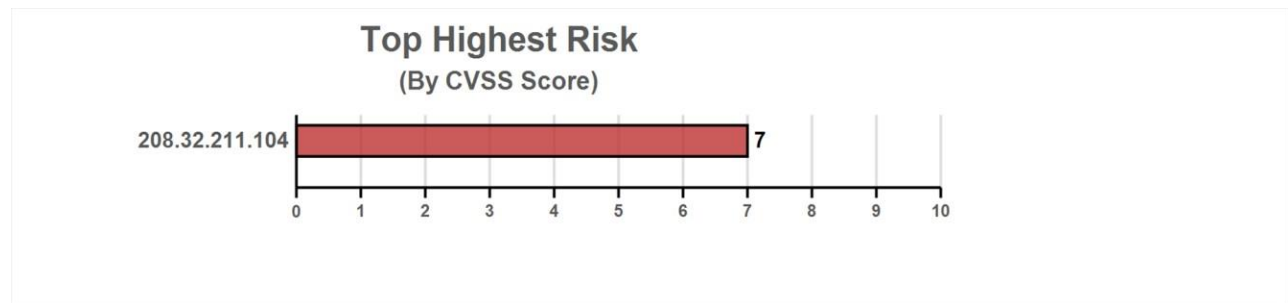
1 - Summary

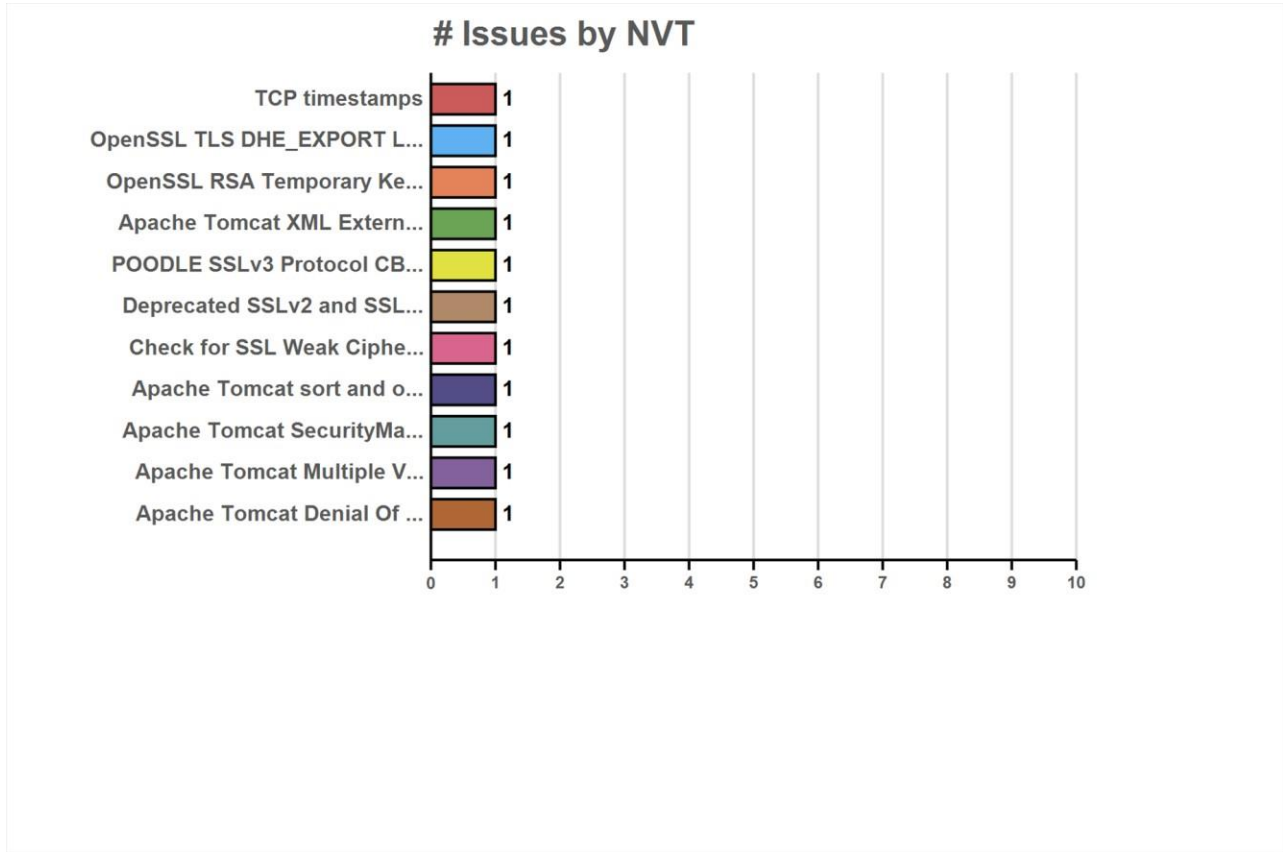
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to mitigate these threats.



Host Issue Summary

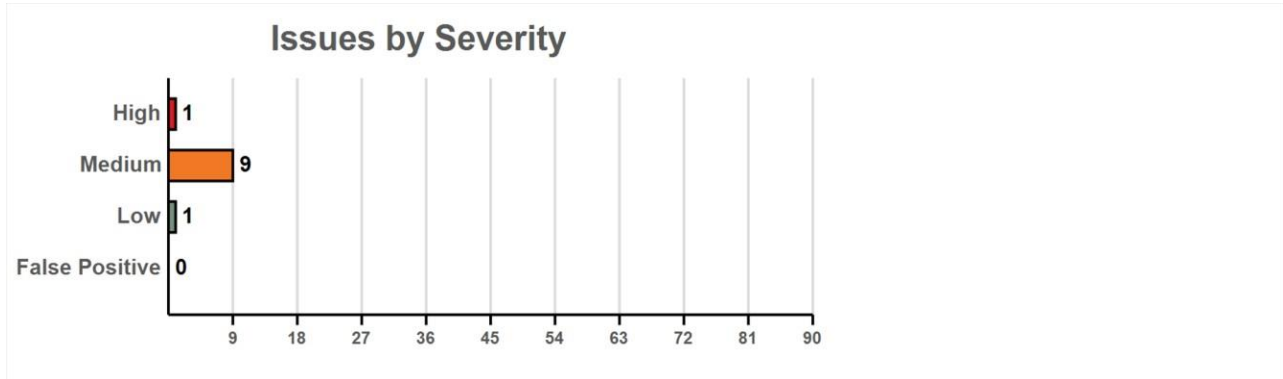
Host	Open Ports	High	Med	Low	False	Highest CVSS
208.32.211.104	2	1	9	1	0	7.8
Total: 1	2	1	9	1	0	7.8



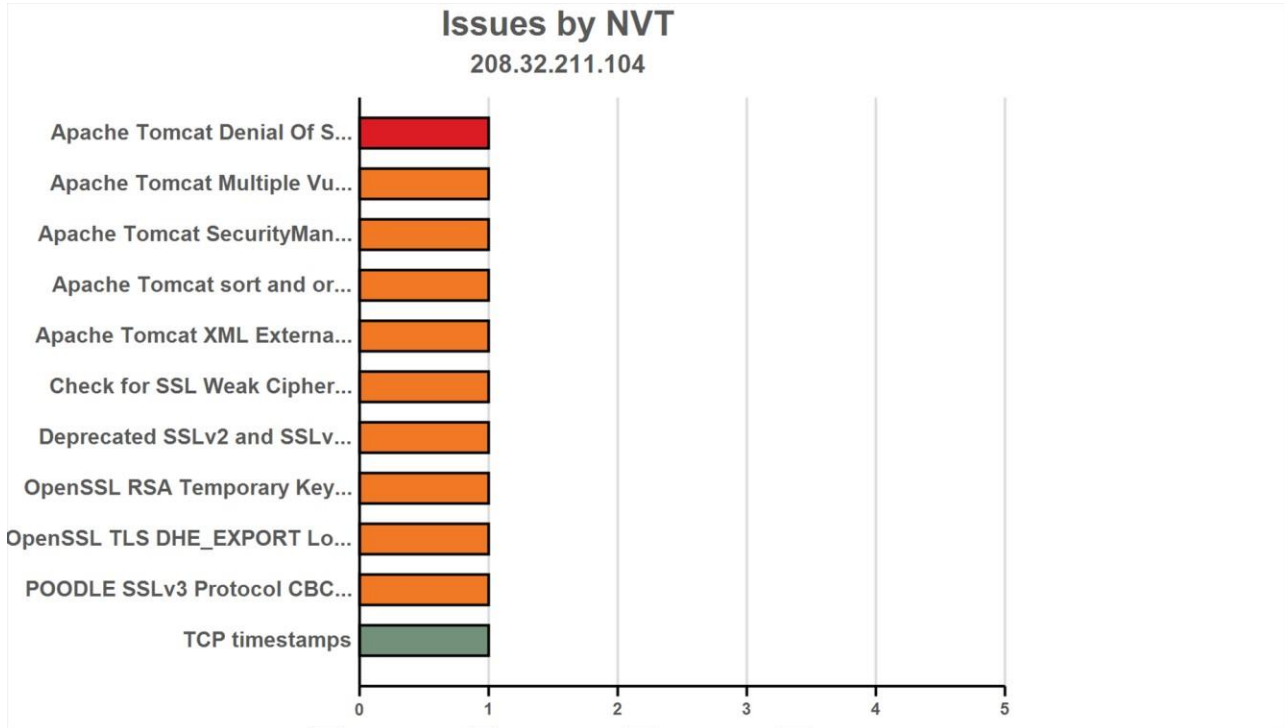


Issue	Count
TCP timestamps	1
OpenSSL TLS DHE_EXPORT LogJam Man in the Middle Security Bypass Vulnerability	1
OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (FREAK)	1
Apache Tomcat XML External Entity Information Disclosure Vulnerability	1
POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability	1
Deprecated SSLv2 and SSLv3 Protocol Detection	1
Check for SSL Weak Ciphers	1
Apache Tomcat sort and orderBy Parameters Cross Site Scripting Vulnerabilities	1
Apache Tomcat SecurityManager Security Bypass Vulnerability -June15 (Linux)	1
Apache Tomcat Multiple Vulnerabilities-01 (Nov14)	1
Apache Tomcat Denial Of Service Vulnerability -June15 (Linux)	1

2 - Scan Details



2.1 - 208.32.211.104



Issue	Count
Apache Tomcat Denial Of Service Vulnerability -June15 (Linux)	1
Apache Tomcat Multiple Vulnerabilities-01 (Nov14)	1
Apache Tomcat SecurityManager Security Bypass Vulnerability -June15 (Linux)	1
Apache Tomcat sort and orderBy Parameters Cross Site Scripting Vulnerabilities	1
Apache Tomcat XML External Entity Information Disclosure Vulnerability	1
Check for SSL Weak Ciphers	1
Deprecated SSLv2 and SSLv3 Protocol Detection	1
OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (FREAK)	1
OpenSSL TLS DHE_EXPORT LogJam Man in the Middle Security Bypass Vulnerability	1
POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability	1
TCP timestamps	1

Host Issue Summary

Host	Open Ports	High	Med	Low	False	Highest CVSS
208.32.211.104	2	1	9	1	0	7.8

Listening Ports

Port
443/tcp (https), 9443/tcp

NVT Issues Summary

Host	Open Ports	High	Med	Low	False	Highest CVSS
Apache Tomcat Denial Of Service Vulnerability -June15 (Linux)	443/tcp (https)	1	0	0	0	7.8
Apache Tomcat Multiple Vulnerabilities-01 (Nov14)	443/tcp (https)	0	1	0	0	5.0
Apache Tomcat SecurityManager Security Bypass Vulnerability - June15 (Linux)	443/tcp (https)	0	1	0	0	5.0
Apache Tomcat sort and orderBy Parameters Cross Site Scripting Vulnerabilities	443/tcp (https)	0	1	0	0	4.3
Check for SSL Weak Ciphers	443/tcp (https)	0	1	0	0	4.3
Deprecated SSLv2 and SSLv3 Protocol Detection	443/tcp (https)	0	1	0	0	4.3
POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability	443/tcp (https)	0	1	0	0	4.3
Apache Tomcat XML External Entity Information Disclosure Vulnerability	443/tcp (https)	0	1	0	0	4.3
OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (FREAK)	443/tcp (https)	0	1	0	0	4.3
OpenSSL TLS DHE_EXPORT LogJam Man in the Middle Security Bypass Vulnerability	443/tcp (https)	0	1	0	0	4.3
TCP timestamps		0	0	1	0	2.6

Security Issues

	High (CVSS: 7.8) NVT: Apache Tomcat Denial Of Service Vulnerability -June15 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.805704)	443/tcp (https)
---	---	-----------------

Summary

This host is installed with Apache Tomcat and is prone to denial of service vulnerability.

Vulnerability Detection Result

Installed version: 6.0.29 Fixed version: 6.0.44

Impact

Successful exploitation will allow remote attackers to conduct denial of service attack. Impact Level: Application

Solution

Upgrade to version 6.0.44 or 7.0.55 or 8.0.9 or later. For updates refer to <http://tomcat.apache.org>

Vulnerability Insight

The flaw is due to improper handling of cases where an HTTP response occurs before finishing the reading of an entire request body

Vulnerability Detection Method


Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: Apache Tomcat Denial Of Service Vulnerability -June15 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.805704) Version used: \$Revision: 1355 \$

Product Detection Result

Product: cpe:/a:apache:tomcat:6.0.29 Method: Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)

References

<http://tomcat.apache.org/security-6.html>, <http://tomcat.apache.org/security-7.html>, <http://openwall.com/lists/oss-security/2015/04/10/1>

	Medium (CVSS: 5) NVT: Apache Tomcat Multiple Vulnerabilities-01 (Nov14) (OID: 1.3.6.1.4.1.25623.1.0.805018)	443/tcp (https)
---	---	-----------------

Summary

This host is running Apache Tomcat and is prone to multiple vulnerabilities.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to cause a denial of service (resource consumption), bypass security-manager restrictions and read arbitrary files, conduct HTTP request smuggling attacks via a crafted Content-Length HTTP header. Impact Level: Application

Solution

Upgrade to version 6.0.40, 7.0.53, 8.0.4 or later. For updates refer to refer <http://tomcat.apache.org>

Vulnerability Insight

Multiple flaws are due to, - An Integer overflow in the parseChunkHeader function in java.org/apache/coyote/http11/filters/ChunkedInputFilter.java - The java.org/apache/catalina/servlets/DefaultServlet.java in the default servlet in does not properly restrict XSLT stylesheets. - Integer overflow in java.org/apache/tomcat/util/buf/Ascii.java in when operated behind a reverse proxy

Vulnerability Detection Method


Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: Apache Tomcat Multiple Vulnerabilities-01 (Nov14) (OID: 1.3.6.1.4.1.25623.1.0.805018) Version used: \$Revision: 1403 \$

Product Detection Result

Product: cpe:/a:apache:tomcat:6.0.29 Method: Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)

References

<http://secunia.com/advisories/60729>, <http://tomcat.apache.org/security-8.html>

	Medium (CVSS: 5) NVT: Apache Tomcat SecurityManager Security Bypass Vulnerability - June15 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.805701)	443/tcp (https)
---	--	-----------------

Summary

This host is installed with Apache Tomcat and is prone to security bypass vulnerability.

Vulnerability Detection Result

Installed version: 6.0.29 Fixed version: 6.0.44

Impact

Successful exploitation will allow remote attackers to bypass certain authentication and obtain sensitive information.
Impact Level: Application

Solution

Upgrade to version 6.0.44 or 7.0.58 or 8.0.16 or later. For updates refer to <http://tomcat.apache.org>

Vulnerability Insight

The flaw is due to the Expression Language does not properly consider the possibility of an accessible interface implemented by an inaccessible class.

Vulnerability Detection Method


Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: Apache Tomcat SecurityManager Security Bypass Vulnerability -June15 (Linux) (OID: 1.3.6.1.4.1.25623.1.0.805701) Version used: \$Revision: 1355 \$

Product Detection Result

Product: cpe:/a:apache:tomcat:6.0.29 Method: Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)

References

<http://tomcat.apache.org/security-6.html>, <http://tomcat.apache.org/security-7.html>, <http://openwall.com/lists/oss-security/2015/04/10/1>

	Medium (CVSS: 4.3) NVT: Apache Tomcat sort and orderBy Parameters Cross Site Scripting Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.103032)	443/tcp (https)
---	--	-----------------

Summary

Apache Tomcat is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

An attacker may leverage these issues to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may let the attacker steal cookie-based authentication credentials and launch other attacks.

Solution

Updates are available please see the references for more information.

Vulnerability Detection Method


Details: Apache Tomcat 'sort' and 'orderBy' Parameters Cross Site Scripting Vulnerabi... (OID: 1.3.6.1.4.1.25623.1.0.103032) Version used: \$Revision: 1224 \$

Product Detection Result

Product: cpe:/a:apache:tomcat:6.0.29 Method: Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)

References

<https://www.securityfocus.com/bid/45015>, <http://tomcat.apache.org/security-6.html>, <http://tomcat.apache.org/security-7.html>, <http://tomcat.apache.org/security-6.html>, <http://tomcat.apache.org/security-7.html>, <http://jakarta.apache.org/tomcat/>, <http://www.securityfocus.com/archive/1/514866>

	Medium (CVSS: 4.3) NVT: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)	443/tcp (https)
---	--	-----------------

Summary

This routine search for weak SSL ciphers offered by a service.

Vulnerability Detection Result

Weak ciphers offered by this service: SSL3_RSA_RC4_40_MD5 SSL3_RSA_RC4_128_MD5
SSL3_RSA_RC4_128_SHA SSL3_RSA_DES_40_CBC_SHA SSL3_RSA_DES_64_CBC_SHA
SSL3_EDH_RSA_DES_40_CBC_SHA SSL3_EDH_RSA_DES_64_CBC_SHA TLS1_RSA_RC4_40_MD5
TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_DES_40_CBC_SHA
TLS1_RSA_DES_64_CBC_SHA TLS1_EDH_RSA_DES_40_CBC_SHA TLS1_EDH_RSA_DES_64_CBC_SHA

Solution


The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength: - Any SSL/TLS using no cipher is considered weak. - All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol. - RC4 is considered to be weak. - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak. - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong

Vulnerability Detection Method

Details: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440) Version used: \$Revision: 733 \$

	Medium (CVSS: 4.3) NVT: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)	443/tcp (https)
---	---	-----------------

Summary

It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Vulnerability Detection Result

In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers.

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Solution

It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

Vulnerability Insight

The SSLv2 and SSLv3 protocols containing known cryptographic flaws.

Vulnerability Detection Method

Check the used protocols of the services provided by this system. Details: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012) Version used: \$Revision: 1183 \$

References

<https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report>, <https://bettercrypto.org/>

	Medium (CVSS: 4.3) NVT: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802087)	443/tcp (https)
---	--	-----------------

Summary

This host is installed with OpenSSL and is prone to information disclosure vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream. Impact Level: Application

Solution

Vendor released a patch to address this vulnerability, For updates contact vendor or refer to <https://www.openssl.org>
NOTE: The only correct way to fix POODLE is to disable SSL v3.0

Vulnerability Insight


The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method

Send a SSLv3 request and check the response. Details: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802087) Version used: \$Revision: 1152 \$

References

<http://osvdb.com/113251>, <https://www.openssl.org/~bodo/ssl-poodle.pdf>,
<https://www.imperialviolet.org/2014/10/14/poodle.html>, <https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html>, <http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html>

	Medium (CVSS: 4.3) NVT: Apache Tomcat XML External Entity Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.805019)	443/tcp (https)
---	--	-----------------

Summary

This host is running Apache Tomcat and is prone to information disclosure vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to read arbitrary files via a crafted web application that provides an XML external entity declaration in conjunction with an entity reference. Impact Level: Application

Solution

Upgrade to version 6.0.40, 7.0.54, 8.0.6 or later. For updates refer to refer <http://tomcat.apache.org>

Vulnerability Insight

The flaw is due to an application does not properly constrain the class loader that accesses the XML parser used with an XSLT stylesheet

Vulnerability Detection Method


Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details: Apache Tomcat XML External Entity Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.805019) Version used: \$Revision: 1403 \$

Product Detection Result

Product: cpe:/a:apache:tomcat:6.0.29 Method: Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)

References

<http://secunia.com/advisories/59732>, <http://tomcat.apache.org/security-7.html>

	Medium (CVSS: 4.3) NVT: OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (FREAK) (OID: 1.3.6.1.4.1.25623.1.0.805142)	443/tcp (https)
---	---	-----------------

Summary

This host is installed with OpenSSL and is prone to man in the middle attack.

Vulnerability Detection Result

EXPORT_RSA cipher suites supported by the remote server: SSLv3:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0014) SSLv3:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0008) SSLv3: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0003)
TLSv1.0: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0014) TLSv1.0:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0008) TLSv1.0: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0003)
TLSv1.1: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0014) TLSv1.1:

TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0008) TLSv1.1: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0003)
TLSv1.2: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0014) TLSv1.2:
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0008) TLSv1.2: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0003)

Impact

Successful exploitation will allow remote attacker to downgrade the security of a session to use EXPORT_RSA ciphers, which are significantly weaker than non-export ciphers. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream. Impact Level: Application

Solution

Remove support for EXPORT_RSA cipher suites from the service. Update to version 0.9.8zd or 1.0.0p or 1.0.1k or later For updates refer to <https://www.openssl.org>

Vulnerability Insight


Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange ciphersuite.

Vulnerability Detection Method

Send a crafted 'Client Hello' request and check the servers response. Details: OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (FREAK) (OID: 1.3.6.1.4.1.25623.1.0.805142) Version used: \$Revision: 1142 \$

References

<https://freakattack.com>, <http://osvdb.org/116794>, <http://secpod.org/blog/?p=3818>,
<http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html>

	Medium (CVSS: 4.3) NVT: OpenSSL TLS DHE_EXPORT LogJam Man in the Middle Security Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.805188)	443/tcp (https)
---	---	-----------------

Summary

This host is installed with OpenSSL and is prone to man in the middle attack.

Vulnerability Detection Result

DHE_EXPORT cipher suites supported by the remote server: TLSv1.0:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0014) TLSv1.1:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0014) TLSv1.2:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0014)

Impact

Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream. Impact Level: Application

Solution

Remove support for DHE_EXPORT cipher suites from the service or Update to version 1.0.2b or 1.0.1n or later, For updates refer to <https://www.openssl.org>

Vulnerability Insight


Flaw is triggered when handling Diffie-Hellman key exchanges defined in the DHE_EXPORT cipher

Vulnerability Detection Method

Send a crafted 'Client Hello' request and check the servers response. Details: OpenSSL TLS 'DHE_EXPORT' LogJam Man in the Middle Security Bypass Vulnerabil... (OID: 1.3.6.1.4.1.25623.1.0.805188) Version used: \$Revision: 1271 \$

References

<https://weakdh.org>, <https://weakdh.org/imperfect-forward-security.pdf>, <http://openwall.com/lists/oss-security/2015/05/20/8>, <https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained>,
<https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes>

	Low (CVSS: 2.6) NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)	
---	--	--

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 1265113531 Paket 2: 1265114641

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: <http://www.microsoft.com/en-us/download/details.aspx?id=9152>

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)
Version used: \$Revision: 787 \$

References

<http://www.ietf.org/rfc/rfc1323.txt>