**Vulnerability Assessment Report**

**For**



**SIPH-nessus**

**April 07, 2022**

**Document Security Level:** Confidential

**Document Version:** 1.0

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Edit Report** | **Editor** |
| 1.0 | April 07, 2022 | Creation | INET Managed Services |

|  |  |  |  |
| --- | --- | --- | --- |
| SIPH-nessus | | INET Managed Services CO., LTD. | |
| Name |  | **Name** |  |
| Position |  | **Position** |  |
| Tel |  | **Tel** |  |
| Signature |  | **Signature** |  |

**Table of Contents**

[1. Restrictions on disclosure and use of information 4](#_Toc98507702)

[2. Operation Method 5](#_Toc98507703)

[3. Project Scope 6](#_Toc98507704)

[3.1 Infrastructure Vulnerability Assessment 6](#_Toc98507705)

[4. Testing Tools 7](#_Toc98507706)

[5. Infrastructure Vulnerability Assessment 7](#_Toc98507707)

[5.1 Target Information 8](#_Toc98507708)

[5.2 Executive summary 9](#_Toc98507709)

[5.2.1 Summary Vulnerability by Severity 9](#_Toc98507710)

[5.2.2 Vulnerability by Target 9](#_Toc98507711)

[5.3 Infrastructure Vulnerability Detail 10](#_Toc98507712)

[6. Appendix 11](#_Toc98507713)

[6.1 About Nessus 11](#_Toc98507714)

[6.1.1 Nessus vulnerabilities 11](#_Toc98507715)

[6.1.2 Nessus risk score 11](#_Toc98507716)

[6.2 About Burp Suite's web vulnerability scanner 13](#_Toc98507717)

[6.2.1 Burp Suite's web vulnerability scanner risk score 13](#_Toc98507718)

# Restrictions on disclosure and use of information

Restriction on Disclosure and Use of Confidential Information. The Executive understands and agrees that the Confidential Information constitutes an asset of the Company and its affiliated entities and may not be converted to the Executive's own use. Accordingly, the Executive hereby agrees that the Executive shall not, directly, or indirectly, at any time, reveal, divulge, or disclose to any Person not expressly authorized by the Company any Confidential Information, and the Executive shall not, directly, or indirectly, use or make use of any Confidential Information in connection with any business activity other than that of the Company. The parties acknowledge and agree that this Agreement is not intended to, and does not, alter either the Company's rights or the Executive's obligations under any state or federal statutory or common law regarding trade secrets and unfair trade.

# Operation Method

* 1. Posture Review
  2. Information Gathering
  3. Enumeration
  4. Vulnerability Assessment
  5. Analyze & Evaluate Risk Value
  6. Report



Figure 1: Operation Method

# Project Scope

## **3.1 Infrastructure Vulnerability Assessment**

**Target / IP Address:**

| **No.** | **Domain / Server Name** | **Public IP Address** | **Private IP Address** | **OS/Model** | **Functions** | **Public Assessment** | **Private Assessment** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | - | - | - | - | - | - | ✓ |

# Testing Tools

|  |  |
| --- | --- |
| **Tool Name** | **Testing Type** |
| Nmap | Host and Service Discovery |
| Nessus Professional | Infrastructure Vulnerability Assessment |
| Burp Suite's web vulnerability scanner | Web Application Vulnerability Assessment |

# Infrastructure Vulnerability Assessment

**Vulnerability Assessment from Public Access (for public target)**

**Testing date:** <<Date SCAN>>

**Tester IP Address:** <<IP Target>>

Diagram

Description automatically generated

Figure 2: Vulnerability Assessment from Public Access

**Vulnerability Assessment from Private Access (for private or restricted access target)**

**Testing date:** <<Date SCAN>>

**Tester IP Address:** Private IP from VPN access

A picture containing diagram

Description automatically generated

Figure 3: Vulnerability Assessment from Private Access

## **5.1 Target Information**

| **No.** | **Domain / Server Name** | **IP Address** | **OS/Model** | **Port** |
| --- | --- | --- | --- | --- |
| 1 | - | 172.28.130.33 | - | TCP: 53, 88, 135, 139, 389, 445, 464, 593, 636, 3268, 3269, 3389 |
| 2 | - | 172.28.130.35 | - | TCP: 25, 80, 81, 88, 135, 139, 443, 444, 445, 465, 587, 593, 808, 1556, 1801, 2103, 2105, 2107, 2525, 3389, 3800, 3801, 3828, 6001, 6667, 9010, 13782 |
| 3 | - | 172.28.130.37 | - | TCP: 25, 80, 81, 135, 139, 443, 444, 445, 465, 587, 593, 808, 1556, 1801, 2103, 2105, 2107, 2525, 3389, 6001, 6646, 6881, 13782 |
| 4 | - | 172.28.130.128 | - | TCP: 21, 135, 139, 445, 2020, 2021, 3389, 6000 |
| 5 | - | 172.28.130.190 | - | TCP: 80, 135, 139, 443, 445, 1433, 3389, 5001, 8009, 8010, 8080, 8081, 8443, 9090, 49152, 49153, 49154 |
| 6 | - | 172.28.131.23 | - | TCP: 22, 80, 427, 443, 902, 5988, 5989, 8000, 8300, 9080 |
| 7 | - | 172.28.131.24 | - | TCP: 22, 80, 443, 3011, 3031, 5432, 8080, 8090, 9090, 9200 |
| 8 | - | 172.28.131.48 | - | TCP: 135, 139, 445, 3389 |
| 9 | - | 172.28.131.49 | - | TCP: 135, 139, 445, 3306, 3389, 4848, 8080, 8181, 10001 |
| 10 | - | 172.28.131.102 | - | TCP: 135, 139, 443, 445, 3389, 4000, 6001, 6101, 7000, 27000, 49152, 49153, 49154, 50002 |
| 11 | - | 172.28.131.105 | - | TCP: 80, 135, 139, 445, 1007, 1010, 1011, 1433, 2007, 3389, 4045, 9998, 49152, 49153, 49154 |
| 12 | - | 172.28.131.108 | - | TCP: 135, 139, 445, 3389, 49152, 49153, 49154, 49155 |
| 13 | - | 172.28.135.188 | - | TCP: 22, 80, 8000 |
| 14 | - | 172.28.135.189 | - | TCP: 135, 139, 445, 1433, 3389, 49152, 49153, 49154, 49155, 49167 |
| 15 | - | 172.28.135.223 | - | TCP: 80, 135, 139, 445, 3389, 5800, 5900, 49152, 49153, 49154, 49155, 49156 |
| 16 | - | 172.28.136.111 | - | TCP: 135, 139, 445, 1556, 2500, 3389, 13782, 49152, 49153, 49154, 49155, 49167, 65000 |
| 17 | - | 172.28.136.118 | - | TCP: 135, 139, 445, 1433, 3211, 3389, 65000 |
| 18 | - | 172.28.136.141 | - | TCP: 135, 139, 445, 3389 |
| 19 | - | 172.28.136.153 | - | TCP: 80, 135, 139, 443, 445, 3389, 49152, 49153, 49154, 49155, 49167 |
| 20 | - | 172.28.137.52 | - | TCP: 22, 111, 1556, 3211, 3301, 6001, 8000, 8001, 8081, 13782 |
| 21 | - | 172.28.137.112 | - | TCP: 22, 1556, 3389, 13782 |
| 22 | - | 172.28.140.41 | - | TCP: 22, 80, 427, 443, 902, 5988, 5989, 8000, 8300, 9080 |
| 23 | - | 172.28.140.43 | - | TCP: 22, 9000 |
| 24 | - | 172.28.140.45 | - | TCP: 22, 81, 443, 8080, 9000 |
| 25 | - | 172.28.188.167 | - | TCP: 22, 443 |
| 26 | - | 172.28.188.168 | - | TCP: 22, 443 |
| 27 | - | 172.28.190.131 | - | TCP: 135, 139, 445, 3389, 49152, 49153, 49154, 49155, 49157, 49167 |
| 28 | - | 172.28.190.133 | - | TCP: 80, 135, 139, 443, 445, 3389, 49152, 49153, 49154, 49155, 49159, 65000 |
| 29 | - | 172.28.190.139 | - | TCP: 80, 443, 3389 |
| 30 | - | 172.28.190.153 | - | TCP: 135, 443, 3389, 5357 |

## **5.2 Executive summary**

The purpose of this activity is to find the vulnerability on the target infrastructure.

### **5.2.1 Summary Vulnerability by Severity**

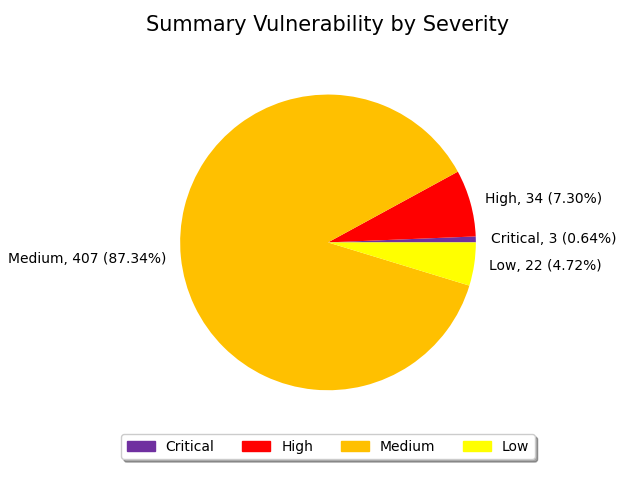


Figure 4: Summary by Severity of Infrastructure Vulnerability Assessment

### **5.2.2 Vulnerability by Target**

| **No.** | **Domain/Server Name** | **IP Address** | **Critical** | **High** | **Medium** | **Low** | **Total** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | - | 172.28.130.33 | 0 | 0 | 13 | 0 | 13 |
| 2 | - | 172.28.130.35 | 0 | 0 | 1 | 0 | 1 |
| 3 | - | 172.28.130.37 | 0 | 0 | 1 | 0 | 1 |
| 4 | - | 172.28.130.128 | 0 | 0 | 12 | 0 | 12 |
| 5 | - | 172.28.130.190 | 1 | 26 | 177 | 2 | 206 |
| 6 | - | 172.28.131.23 | 0 | 3 | 11 | 1 | 15 |
| 7 | - | 172.28.131.24 | 0 | 1 | 14 | 4 | 19 |
| 8 | - | 172.28.131.48 | 0 | 0 | 6 | 0 | 6 |
| 9 | - | 172.28.131.49 | 0 | 0 | 9 | 1 | 10 |
| 10 | - | 172.28.131.102 | 0 | 0 | 20 | 2 | 22 |
| 11 | - | 172.28.131.105 | 0 | 0 | 18 | 0 | 18 |
| 12 | - | 172.28.131.108 | 0 | 0 | 10 | 1 | 11 |
| 13 | - | 172.28.135.188 | 0 | 0 | 1 | 0 | 1 |
| 14 | - | 172.28.135.189 | 1 | 0 | 10 | 1 | 12 |
| 15 | - | 172.28.135.223 | 1 | 0 | 16 | 1 | 18 |
| 16 | - | 172.28.136.111 | 0 | 0 | 10 | 1 | 11 |
| 17 | - | 172.28.136.118 | 0 | 0 | 8 | 0 | 8 |
| 18 | - | 172.28.136.141 | 0 | 0 | 4 | 0 | 4 |
| 19 | - | 172.28.136.153 | 0 | 0 | 9 | 0 | 9 |
| 20 | - | 172.28.137.52 | 0 | 0 | 4 | 0 | 4 |
| 21 | - | 172.28.137.112 | 0 | 0 | 1 | 0 | 1 |
| 22 | - | 172.28.140.41 | 0 | 4 | 8 | 0 | 12 |
| 23 | - | 172.28.140.43 | 0 | 0 | 0 | 0 | 0 |
| 24 | - | 172.28.140.45 | 0 | 0 | 7 | 0 | 7 |
| 25 | - | 172.28.188.167 | 0 | 0 | 3 | 3 | 6 |
| 26 | - | 172.28.188.168 | 0 | 0 | 4 | 3 | 7 |
| 27 | - | 172.28.190.131 | 0 | 0 | 9 | 1 | 10 |
| 28 | - | 172.28.190.133 | 0 | 0 | 8 | 0 | 8 |
| 29 | - | 172.28.190.139 | 0 | 0 | 8 | 1 | 9 |
| 30 | - | 172.28.190.153 | 0 | 0 | 5 | 0 | 5 |
| **Total** | | | 3 | 34 | 407 | 22 | 466 |

## **5.3 Infrastructure Vulnerability Detail**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 1 | **Finding** | Microsoft SQL Server Unsupported Version Detection (remote check) |
| **Severity** | **Critical** | **Port** | TCP: 1433, 53884 |
| **Target** | 172.28.130.190(1433), 172.28.135.189(1433), 172.28.135.223(53884) | | |
| **Detail** | According to its self-reported version number, the installation of Microsoft SQL Server on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. | | |
| **Solution** | Upgrade to a version of Microsoft SQL Server that is currently supported. | | |
| **Remark** | http://www.nessus.org/u?d4418a57 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 2 | **Finding** | Unsupported Web Server Detection |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities. | | |
| **Solution** | Remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 3 | **Finding** | Apache Tomcat 7.x 7.0.21 Arbitrary AJP Message Control |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.x listening on the remote host is prior to 7.0.21. It is, therefore, affected by a vulnerability that allows an attacker to have  control over AJP messages. Specially crafted requests are incorrectly processed by Tomcat and can cause the server to allow injection of arbitrary AJP messages. This can lead to an authentication bypass and the disclosure of sensitive information. Note that this vulnerability only occurs when the following are true :  - the org.apache.jk.server.JkCoyoteHandler AJP connector  is not used.  - POST requests are accepted.  - the request body is not processed. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.21 or later. | | |
| **Remark** | https://bz.apache.org/bugzilla/show\_bug.cgi?id=51698 http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.21 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 4 | **Finding** | Apache Tomcat 7.0.x 7.0.52 Content-Type DoS |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.0.x listening on the remote host is prior to 7.0.52. It is, therefore, affected by an error related to handling 'Content-Type' HTTP headers and multipart requests such as file uploads. Note that this error exists because of the bundled version of Apache Commons FileUpload. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Update to Apache Tomcat version 7.0.52 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.52 http://www.nessus.org/u?358ef049 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 5 | **Finding** | Apache Tomcat 7.0.x 7.0.57 Multiple Vulnerabilities (POODLE) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat service listening on the remote host is 7.0.x prior to 7.0.57. It is, therefore, affected by the following vulnerabilities :  - A memory double-free error exists in 'd1\_both.c' related  to handling DTLS packets that allows denial of service  attacks. (CVE-2014-3505)  - An unspecified error exists in 'd1\_both.c' related to  handling DTLS handshake messages that allows denial of  service attacks due to large amounts of memory being  consumed. (CVE-2014-3506)  - A memory leak error exists in 'd1\_both.c' related to  handling specially crafted DTLS packets that allows  denial of service attacks. (CVE-2014-3507)  - An error exists in the 'OBJ\_obj2txt' function when  various 'X509\_name\_\*' pretty printing functions are  used, which leak process stack data, resulting in an  information disclosure. (CVE-2014-3508)  - An error exists related to 'ec point format extension'  handling and multithreaded clients that allows freed  memory to be overwritten during a resumed session.  (CVE-2014-3509)  - A NULL pointer dereference error exists related to  handling anonymous ECDH cipher suites and crafted  handshake messages that allows denial of service attacks  against clients. (CVE-2014-3510)  - An error exists related to handling fragmented  'ClientHello' messages that allows a man-in-the-middle  attacker to force usage of TLS 1.0 regardless of higher  protocol levels being supported by both the server and  the client. (CVE-2014-3511)  - Buffer overflow errors exist in 'srp\_lib.c' related to  handling Secure Remote Password protocol (SRP)  parameters, which can allow a denial of service or have  other unspecified impact. (CVE-2014-3512)  - A memory leak issue exists in 'd1\_srtp.c' related to  the DTLS SRTP extension handling and specially crafted  handshake messages that can allow denial of service  attacks. (CVE-2014-3513)  - An error exists related to the way SSL 3.0 handles  padding bytes when decrypting messages encrypted using  block ciphers in cipher block chaining (CBC) mode.  Man-in-the-middle attackers can decrypt a selected byte  of a cipher text in as few as 256 tries if they are able  to force a victim application to repeatedly send the  same data over newly created SSL 3.0 connections. This  is also known as the 'POODLE' issue. (CVE-2014-3566)  - A memory leak issue exists in 't1\_lib.c' related to  session ticket handling that can allow denial of service  attacks. (CVE-2014-3567)  - An error exists related to the build configuration  process and the 'no-ssl3' build option that allows  servers and clients to process insecure SSL 3.0  handshake messages. (CVE-2014-3568)  - A NULL pointer dereference error exists in 't1\_lib.c',  related to handling Secure Remote Password protocol  (SRP) ServerHello messages, which allows a malicious  server to crash a client, resulting in a denial of  service. (CVE-2014-5139) Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Update to Apache Tomcat version 7.0.57 or later. | | |
| **Remark** | http://tomcat.apache.org/tomcat-7.0-doc/changelog.html https://www.imperialviolet.org/2014/10/14/poodle.html https://www.openssl.org/~bodo/ssl-poodle.pdf https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 6 | **Finding** | Apache Tomcat 6.0.x 6.0.48 / 7.0.x 7.0.73 / 8.0.x 8.0.39 / 8.5.x 8.5.8 / 9.0.x 9.0.0.M13 Multiple Vulnerabilities |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat service running on the remote host is 6.0.x prior to 6.0.48, 7.0.x prior to 7.0.73, 8.0.x prior to 8.0.39, 8.5.x prior to 8.5.8, or 9.0.x prior to 9.0.0.M13. It is, therefore, affected by multiple  vulnerabilities :  - A flaw exists that is triggered when handling request  lines containing certain invalid characters. An   unauthenticated, remote attacker can exploit this, by  injecting additional headers into responses, to conduct  HTTP response splitting attacks. (CVE-2016-6816)  - A denial of service vulnerability exists in the HTTP/2  parser due to an infinite loop caused by improper  parsing of overly large headers. An unauthenticated,  remote attacker can exploit this, via a specially  crafted request, to cause a denial of service condition.  Note that this vulnerability only affects 8.5.x  versions. (CVE-2016-6817)  - A remote code execution vulnerability exists in the JMX  listener in JmxRemoteLifecycleListener.java due to  improper deserialization of Java objects. An  unauthenticated, remote attacker can exploit this to  execute arbitrary code. (CVE-2016-8735) Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 6.0.48 / 7.0.73 / 8.0.39 / 8.5.8 / 9.0.0.M13 or later. | | |
| **Remark** | http://www.nessus.org/u?1e8a81e1 http://www.nessus.org/u?1c7e7b23 http://www.nessus.org/u?833cb56a http://www.nessus.org/u?87d6ed56 http://www.nessus.org/u?5f7bb039 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 7 | **Finding** | Apache Tomcat 8.5.0 8.5.32 Multiple Vulnerabilities |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 8.5.x prior to 8.5.32. It is, therefore, affected by multiple vulnerabilities. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.32 or later. | | |
| **Remark** | http://www.nessus.org/u?5070a438 http://www.nessus.org/u?d5ab19d6 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 8 | **Finding** | Apache Tomcat 7.0.x 7.0.70 / 8.0.x 8.0.36 / 8.5.x 8.5.3 / 9.0.x 9.0.0.M8 Denial of Service |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat instance listening on the remote host is 7.0.x prior to 7.0.70, 8.0.x 8.0.36, 8.5.x 8.5.3 or 9.0.x 9.0.0.M8. It is, therefore, affected by a denial of service vulnerability:  - A denial of service vulnerability was identified in  Commons FileUpload that occurred when the length of the  multipart boundary was just below the size of the buffer  (4096 bytes) used to read the uploaded file if the  boundary was the typical tens of bytes long. Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.70 / 8.0.36 / 8.5.3 / 9.0.0.M8 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.70 http://www.nessus.org/u?ecb3da27 http://tomcat.apache.org/security-9.html#Fixed\_in\_Apache\_Tomcat\_9.0.0.M8 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 9 | **Finding** | Apache Tomcat 7.0.x 7.0.100 / 8.5.x 8.5.51 / 9.0.x 9.0.31 Multiple Vulnerabilities |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8081, 8443, 8444 |
| **Target** | 172.28.130.190(443, 8080, 8081, 8443, 8444) | | |
| **Detail** | The version of Tomcat installed on the remote host is 7.0.x prior to 7.0.100, 8.x prior to 8.5.51, or 9.0.x prior to 9.0.31. It is, therefore, affected by multiple vulnerabilities.  - An HTTP request smuggling vulnerability exists in Tomcat due to mishandling Transfer-Encoding headers  behind a reverse proxy. An unauthenticated, remote attacker can exploit this, via crafted HTTP requests,  to cause unintended HTTP requests to reach the back-end. (CVE-2019-17569)  - An HTTP request smuggling vulnerability exists in Tomcat due to bad end-of-line (EOL) parsing that allowed  some invalid HTTP headers to be parsed as valid. An unauthenticated, remote attacker can exploit this, via  crafted HTTP requests, to cause unintended HTTP requests to reach the back-end. (CVE-2020-1935)  - An arbitrary file read vulnerability exists in Tomcat's Apache JServ Protocol (AJP) due to an  implementation defect. A remote, unauthenticated attacker could exploit this to access files which, under  normal conditions, would be restricted. If the Tomcat instance supports file uploads, the vulnerability  could also be leveraged to achieve remote code execution. (CVE-2020-1938) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version  number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.100, 8.5.51, 9.0.31 or later. | | |
| **Remark** | https://www.cnvd.org.cn/webinfo/show/5415 http://www.nessus.org/u?8ebe6246 http://www.nessus.org/u?4e287adb http://www.nessus.org/u?cbc3d54e | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 10 | **Finding** | Apache Tomcat AJP Connector Request Injection (Ghostcat) |
| **Severity** | **High** | **Port** | TCP: 8009 |
| **Target** | 172.28.130.190(8009) | | |
| **Detail** | A file read/inclusion vulnerability was found in AJP connector. A  remote, unauthenticated attacker could exploit this vulnerability to  read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload  malicious JavaServer Pages (JSP) code within a variety of file types  and gain remote code execution (RCE). | | |
| **Solution** | Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later. | | |
| **Remark** | http://www.nessus.org/u?8ebe6246 http://www.nessus.org/u?4e287adb http://www.nessus.org/u?cbc3d54e https://access.redhat.com/security/cve/CVE-2020-1745 https://access.redhat.com/solutions/4851251 http://www.nessus.org/u?dd218234 http://www.nessus.org/u?dd772531 http://www.nessus.org/u?2a01d6bf http://www.nessus.org/u?3b5af27e http://www.nessus.org/u?9dab109f http://www.nessus.org/u?5eafcf70 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 11 | **Finding** | ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2018-0027) (Remote Check) |
| **Severity** | **High** | **Port** | TCP: 443 |
| **Target** | 172.28.131.23(443), 172.28.140.41(443) | | |
| **Detail** | The remote VMware ESXi host is version 6.0, 6.5, or 6.7 and is missing a security patch. It is, therefore, vulnerable to multiple vulnerabilities. Leveraging the most severe of these vulnerabilities could allow an attacker to execute arbitrary code on the host from the security context of an unprivileged user on the guest system. Note: CVE-2018-6982 only applies to ESXi 6.5 and 6.7 installations.  ESXi 6.0 installations are not affected. | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2018-0027.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 12 | **Finding** | ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0005) (Remote Check) |
| **Severity** | **High** | **Port** | TCP: 443 |
| **Target** | 172.28.131.23(443), 172.28.140.41(443) | | |
| **Detail** | The remote VMware ESXi host is version 6.0, 6.5, or 6.7 and is missing a security patch. It is, therefore, vulnerable to multiple vulnerabilities, including:  - An out-of-bounds read/write vulnerability and a Time-of-check  Time-of-use (TOCTOU) vulnerability in the virtual USB 1.1 UHCI  (Universal Host Controller Interface). Exploitation of these  issues requires an attacker to have access to a virtual machine  with a virtual USB controller present. These issues may allow a  guest to execute code on the host. (CVE-2019-5518, CVE-2019-5519) | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2019-0005.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 13 | **Finding** | ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026) |
| **Severity** | **High** | **Port** | TCP: 443 |
| **Target** | 172.28.131.23(443), 172.28.140.41(443) | | |
| **Detail** | According to its self-reported version number, the remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by multiple vulnerabilities.   - A use-after-free error exists in the XHCI USB controller. An unauthenticated, local attacker with local  administrative privileges on a virtual machine can exploit this, to execute code as the virtual machine's  VMX process running on the host. (CVE-2020-4004)  - A privilege escalation vulnerability exists in ESXi due to how certain system calls are managed. An  authenticated, local attacker with privileges within the VPM process can exploit this, when chained with  CVE-2020-4004, to obtain escalated privileges. (CVE-2020-4005) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2020-0026.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 14 | **Finding** | SSL Version 2 and 3 Protocol Detection |
| **Severity** | **High** | **Port** | TCP: 3031 |
| **Target** | 172.28.131.24(3031) | | |
| **Detail** | The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:  - An insecure padding scheme with CBC ciphers.  - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients. Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely. NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'. | | |
| **Solution** | Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead. | | |
| **Remark** | https://www.schneier.com/academic/paperfiles/paper-ssl.pdf http://www.nessus.org/u?b06c7e95 http://www.nessus.org/u?247c4540 https://www.openssl.org/~bodo/ssl-poodle.pdf http://www.nessus.org/u?5d15ba70 https://www.imperialviolet.org/2014/10/14/poodle.html https://tools.ietf.org/html/rfc7507 https://tools.ietf.org/html/rfc7568 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 15 | **Finding** | ESXi 6.0 / 6.5 / 6.7 Out-of-Bounds Read Vulnerability (VMSA-2018-0026) (Remote Check) |
| **Severity** | **High** | **Port** | TCP: 443 |
| **Target** | 172.28.140.41(443) | | |
| **Detail** | The remote VMware ESXi host is version 6.0, 6.5, or 6.7 and is missing a security patch. It is, therefore, vulnerable to an out-of-bounds read vulnerability in SVGA devices. An attacker with access to a guest system may be able to execute code on the host system by leveraging this vulnerability. | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2018-0026.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 16 | **Finding** | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| **Severity** | **Medium** | **Port** | TCP: 443, 636, 1433, 3031, 3269, 3389, 6001, 6101, 8443, 10102, 53884 |
| **Target** | 172.28.130.33(636, 3269, 3389), 172.28.130.128(3389), 172.28.130.190(8443), 172.28.131.24(3031), 172.28.131.48(3389), 172.28.131.49(3389, 10102), 172.28.131.102(6001, 6101), 172.28.131.105(1433, 3389), 172.28.131.108(3389), 172.28.135.223(3389, 53884), 172.28.136.111(3389), 172.28.136.153(443), 172.28.188.167(443), 172.28.188.168(443), 172.28.190.131(3389), 172.28.190.133(3389), 172.28.190.139(3389) | | |
| **Detail** | The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or  else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network. | | |
| **Solution** | Reconfigure the affected application if possible to avoid use of medium strength ciphers. | | |
| **Remark** | https://www.openssl.org/blog/blog/2016/08/24/sweet32/ https://sweet32.info | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 17 | **Finding** | SSL Certificate with Wrong Hostname |
| **Severity** | **Medium** | **Port** | TCP: 443, 636, 1433, 3269, 3389, 8443, 8444, 50266, 53884 |
| **Target** | 172.28.130.33(636, 3269, 3389), 172.28.130.128(3389), 172.28.130.190(443, 1433, 3389, 8443, 8444), 172.28.131.48(3389), 172.28.131.102(443, 3389, 50266), 172.28.131.105(1433, 3389), 172.28.131.108(3389), 172.28.135.189(1433, 3389), 172.28.135.223(53884), 172.28.136.111(3389), 172.28.136.118(1433, 3389), 172.28.136.141(3389), 172.28.136.153(443, 3389), 172.28.190.133(443) | | |
| **Detail** | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. | | |
| **Solution** | Purchase or generate a proper SSL certificate for this service. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 18 | **Finding** | SSL Certificate Cannot Be Trusted |
| **Severity** | **Medium** | **Port** | TCP: 443, 636, 1433, 3031, 3041, 3269, 3389, 4300, 5007, 5989, 6001, 6101, 8080, 8181, 8443, 8444, 9080, 9090, 9400, 10102, 50266, 53884 |
| **Target** | 172.28.130.33(636, 3269, 3389), 172.28.130.128(3389), 172.28.130.190(443, 1433, 3389, 8443, 8444), 172.28.131.23(443, 5989, 9080), 172.28.131.24(443, 3031, 9090, 9400), 172.28.131.48(3389), 172.28.131.49(3389, 8181, 10102), 172.28.131.102(443, 3389, 6001, 6101, 50266), 172.28.131.105(1433, 3041, 3389, 8444), 172.28.131.108(3389), 172.28.135.189(1433, 3389), 172.28.135.223(3389, 53884), 172.28.136.111(3389), 172.28.136.118(1433, 3389), 172.28.136.141(3389), 172.28.136.153(3389), 172.28.137.52(4300), 172.28.140.41(443, 5989, 9080), 172.28.140.45(443, 8080), 172.28.188.167(443), 172.28.188.168(443, 5007), 172.28.190.131(3389), 172.28.190.133(3389), 172.28.190.139(3389), 172.28.190.153(443, 3389) | | |
| **Detail** | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :  - First, the top of the certificate chain sent by the  server might not be descended from a known public  certificate authority. This can occur either when the  top of the chain is an unrecognized, self-signed  certificate, or when intermediate certificates are  missing that would connect the top of the certificate  chain to a known public certificate authority.  - Second, the certificate chain may contain a certificate  that is not valid at the time of the scan. This can  occur either when the scan occurs before one of the  certificate's 'notBefore' dates, or after one of the  certificate's 'notAfter' dates.  - Third, the certificate chain may contain a signature  that either didn't match the certificate's information  or could not be verified. Bad signatures can be fixed by  getting the certificate with the bad signature to be  re-signed by its issuer. Signatures that could not be  verified are the result of the certificate's issuer  using a signing algorithm that Nessus either does not  support or does not recognize. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and  identity of the web server. This could make it easier to carry out  man-in-the-middle attacks against the remote host. | | |
| **Solution** | Purchase or generate a proper SSL certificate for this service. | | |
| **Remark** | https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 19 | **Finding** | SSL Self-Signed Certificate |
| **Severity** | **Medium** | **Port** | TCP: 443, 1433, 3041, 3389, 4300, 8080, 8443, 8444, 9080, 9400, 10102, 50266, 53884 |
| **Target** | 172.28.130.33(3389), 172.28.130.128(3389), 172.28.130.190(443, 1433, 3389, 8443, 8444), 172.28.131.23(443, 9080), 172.28.131.24(9400), 172.28.131.48(3389), 172.28.131.49(3389, 10102), 172.28.131.102(443, 3389, 50266), 172.28.131.105(1433, 3041, 3389, 8444), 172.28.131.108(3389), 172.28.135.189(1433, 3389), 172.28.135.223(3389, 53884), 172.28.136.111(3389), 172.28.136.118(1433, 3389), 172.28.136.141(3389), 172.28.136.153(3389), 172.28.137.52(4300), 172.28.140.41(9080), 172.28.140.45(443, 8080), 172.28.190.131(3389), 172.28.190.133(3389), 172.28.190.139(3389), 172.28.190.153(3389) | | |
| **Detail** | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. | | |
| **Solution** | Purchase or generate a proper SSL certificate for this service. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 20 | **Finding** | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
| **Severity** | **Medium** | **Port** | TCP: 443, 1433, 3031, 3389, 53884 |
| **Target** | 172.28.130.128(3389), 172.28.131.24(3031), 172.28.131.105(1433, 3389), 172.28.131.108(3389), 172.28.135.223(3389, 53884), 172.28.136.111(3389), 172.28.136.153(443), 172.28.190.131(3389), 172.28.190.133(3389), 172.28.190.139(3389) | | |
| **Detail** | The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext. | | |
| **Solution** | Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support. | | |
| **Remark** | https://www.rc4nomore.com/ http://www.nessus.org/u?ac7327a0 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ https://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 21 | **Finding** | TLS Version 1.0 Protocol Detection |
| **Severity** | **Medium** | **Port** | TCP: 443, 636, 1433, 3031, 3269, 3389, 4300, 5989, 6001, 6101, 8080, 8443, 8444, 9080, 10102, 50266, 53884 |
| **Target** | 172.28.130.33(636, 3269, 3389), 172.28.130.128(3389), 172.28.130.190(1433, 3389, 8443, 8444), 172.28.131.23(443, 5989, 9080), 172.28.131.24(3031), 172.28.131.48(3389), 172.28.131.49(3389, 10102), 172.28.131.102(443, 3389, 6001, 6101, 50266), 172.28.131.105(1433, 3389, 8444), 172.28.131.108(3389), 172.28.135.189(1433, 3389), 172.28.135.223(3389, 53884), 172.28.136.111(3389), 172.28.136.118(1433, 3389), 172.28.136.141(3389), 172.28.136.153(443, 3389), 172.28.137.52(4300), 172.28.140.45(443, 8080), 172.28.190.131(3389), 172.28.190.133(443, 3389), 172.28.190.139(3389), 172.28.190.153(443, 3389) | | |
| **Detail** | The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.  As of March 31, 2020, Endpoints that aren’t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.  PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits. | | |
| **Solution** | Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0. | | |
| **Remark** | https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 22 | **Finding** | web.config File Information Disclosure |
| **Severity** | **Medium** | **Port** | TCP: 2020 |
| **Target** | 172.28.130.128(2020) | | |
| **Detail** | An information disclosure vulnerability exists in the remote web server due to the disclosure of the web.config file. An unauthenticated, remote attacker can exploit this, via a simple GET request, to disclose potentially sensitive configuration information. | | |
| **Solution** | Ensure proper restrictions are in place, or remove the web.config file if the file is not required. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 23 | **Finding** | PHP 7.4.x 7.4.18 / 8.x 8.0.5 Integer Overflow |
| **Severity** | **Medium** | **Port** | TCP: 2021 |
| **Target** | 172.28.130.128(2021) | | |
| **Detail** | The version of PHP installed on the remote host is 7.4.x prior to 7.4.18, or 8.x prior to 8.0.5. It is, therefore, affected by an integer overflow condition in pnctl\_exec(). An attacker can exploit this to cause a denial of service (DoS) condition or the execution of arbitrary code. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported  version | | |
| **Solution** | Upgrade to PHP version 7.4.18, 8.0.5 or later. | | |
| **Remark** | https://www.php.net/ChangeLog-7.php#7.4.18 https://www.php.net/ChangeLog-8.php#8.0.5 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 24 | **Finding** | PHP 7.4.x 7.4.25 |
| **Severity** | **Medium** | **Port** | TCP: 2021 |
| **Target** | 172.28.130.128(2021) | | |
| **Detail** | The version of PHP installed on the remote host is prior to 7.4.25. It is, therefore, affected by a vulnerability as referenced in the Version 7.4.25 advisory.  - In PHP versions 7.3.x up to and including 7.3.31, 7.4.x below 7.4.25 and 8.0.x below 8.0.12, when running  PHP FPM SAPI with main FPM daemon process running as root and child worker processes running as lower-  privileged users, it is possible for the child processes to access memory shared with the main process and  write to it, modifying it in a way that would cause the root process to conduct invalid memory reads and  writes, which can be used to escalate privileges from local unprivileged user to the root user.  (CVE-2021-21703) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to PHP version 7.4.25 or later. | | |
| **Remark** | http://bugs.php.net/81026 http://php.net/ChangeLog-7.php#7.4.25 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 25 | **Finding** | PHP 7.4.x 7.4.24 Arbitrary File Write |
| **Severity** | **Medium** | **Port** | TCP: 2021 |
| **Target** | 172.28.130.128(2021) | | |
| **Detail** | The version of PHP installed on the remote host is 7.4.x prior to 7.4.25. It is, therefore, affected by a vulnerability as referenced in the version 7.4.24 advisory. In the Microsoft Windows environment, ZipArchive::extractTo may be tricked into writing a file outside target directory when extracting a ZIP file, thus potentially causing files to be created or overwritten, subject to OS permissions. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to PHP version 7.4.24 or later. | | |
| **Remark** | http://bugs.php.net/81420 http://php.net/ChangeLog-7.php#7.4.24 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 26 | **Finding** | PHP 7.4.x 7.4.26 |
| **Severity** | **Medium** | **Port** | TCP: 2021 |
| **Target** | 172.28.130.128(2021) | | |
| **Detail** | The version of PHP installed on the remote host is prior to 7.4.26. It is, therefore, affected by a vulnerability as referenced in the Version 7.4.26 advisory.  - In PHP versions 7.3.x below 7.3.33, 7.4.x below 7.4.26 and 8.0.x below 8.0.13, certain XML parsing  functions, like simplexml\_load\_file(), URL-decode the filename passed to them. If that filename contains  URL-encoded NUL character, this may cause the function to interpret this as the end of the filename, thus  interpreting the filename differently from what the user intended, which may lead it to reading a  different file than intended. (CVE-2021-21707) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to PHP version 7.4.26 or later. | | |
| **Remark** | http://bugs.php.net/79971 http://php.net/ChangeLog-7.php#7.4.26 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 27 | **Finding** | PHP 7.4.x 7.4.28 |
| **Severity** | **Medium** | **Port** | TCP: 2021 |
| **Target** | 172.28.130.128(2021) | | |
| **Detail** | The version of PHP installed on the remote host is prior to 7.4.28. It is, therefore, affected by a vulnerability as referenced in the Version 7.4.28 advisory.  - In PHP versions 7.4.x below 7.4.28, 8.0.x below 8.0.16, and 8.1.x below 8.1.3, when using filter functions  with FILTER\_VALIDATE\_FLOAT filter and min/max limits, if the filter fails, there is a possibility to  trigger use of allocated memory after free, which can result it crashes, and potentially in overwrite of  other memory chunks and RCE. This issue affects: code that uses FILTER\_VALIDATE\_FLOAT with min/max limits.  (CVE-2021-21708) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to PHP version 7.4.28 or later. | | |
| **Remark** | http://php.net/ChangeLog-7.php#7.4.28 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 28 | **Finding** | Apache Tomcat Default Files |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8081, 8443, 8444 |
| **Target** | 172.28.130.190(443, 8080, 8081, 8443, 8444) | | |
| **Detail** | The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself. | | |
| **Solution** | Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to  replace or modify the default error page. | | |
| **Remark** | http://www.nessus.org/u?4cb3b4dd https://www.owasp.org/index.php/Securing\_tomcat | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 29 | **Finding** | SSL Certificate Expiry |
| **Severity** | **Medium** | **Port** | TCP: 3031, 8444 |
| **Target** | 172.28.130.190(8444), 172.28.131.24(3031) | | |
| **Detail** | This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired. | | |
| **Solution** | Purchase or generate a new SSL certificate to replace the existing one. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 30 | **Finding** | SSL Certificate Signed Using Weak Hashing Algorithm |
| **Severity** | **Medium** | **Port** | TCP: 1433, 3031, 8443, 53884 |
| **Target** | 172.28.130.190(1433, 8443), 172.28.131.24(3031), 172.28.131.105(1433), 172.28.135.189(1433), 172.28.135.223(53884) | | |
| **Detail** | The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm. Note that certificates in the chain that are contained in the Nessus CA database (known\_CA.inc) have been ignored. | | |
| **Solution** | Contact the Certificate Authority to have the SSL certificate reissued. | | |
| **Remark** | https://tools.ietf.org/html/rfc3279 http://www.nessus.org/u?9bb87bf2 http://www.nessus.org/u?e120eea1 http://www.nessus.org/u?5d894816 http://www.nessus.org/u?51db68aa http://www.nessus.org/u?9dc7bfba | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 31 | **Finding** | Apache Tomcat Cross-Application File Manipulation |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the remote host is running a vulnerable version of Apache Tomcat. Affected versions permit a web application to replace the XML parser used to process the XML and TLD files of other applications. This could allow a malicious web app to read or modify 'web.xml', 'context.xml', or TLD files of arbitrary web applications. | | |
| **Solution** | Upgrade to versions 7.0.19 / 6.0.20 / 5.5.28 / 4.1.40 or later. Alternatively, apply the patches referenced in the vendor advisory. | | |
| **Remark** | https://bz.apache.org/bugzilla/show\_bug.cgi?id=29936 https://www.securityfocus.com/archive/1/504090 http://tomcat.apache.org/security-6.html http://tomcat.apache.org/security-5.html http://tomcat.apache.org/security-4.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 32 | **Finding** | Apache Tomcat 6.x 6.0.30 / 7.x 7.0.5 Multiple XSS |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat listening on the remote host is 6.x prior to 6.0.30 or 7.x prior to 7.0.5. It is, therefore, affected by multiple cross-site scripting vulnerabilities in the Tomcat Manager application's 'sessionList.jsp' file. The 'sort' and 'orderby' parameters are not properly sanitized before being returned to the user and can be used to inject arbitrary script into the user's browser. Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. Also note, in the case of Tomcat 7.x, successful exploitation requires that the cross-site request forgery (CSRF) filter is disabled. | | |
| **Solution** | Update Apache Tomcat to version 6.0.30 / 7.0.5 or later. | | |
| **Remark** | https://seclists.org/fulldisclosure/2010/Nov/283 http://tomcat.apache.org/security-6.html#Fixed\_in\_Apache\_Tomcat\_6.0.30 http://www.nessus.org/u?37871cd8 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 33 | **Finding** | Apache Tomcat 7.x 7.0.4 SecurityManager Local Security Bypass |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.x listening on the remote host is prior to 7.0.4. It is, therefore, affected by a security bypass vulnerability due to an error in the access restriction on a 'ServletContext' attribute which holds the location of the work directory in Tomcat's SecurityManager. A malicious web application can modify the location of the working directory which then allows improper read and write access to arbitrary files and directories in the context of Tomcat. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.4 or later. Alternatively, undeploy untrusted third-party web applications. | | |
| **Remark** | http://www.nessus.org/u?8da12114 https://seclists.org/fulldisclosure/2011/Feb/74 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 34 | **Finding** | Apache Tomcat 7.x 7.0.6 Manager Interface XSS |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.x listening on the remote host is prior to 7.0.6. It is, therefore, affected by a cross-site scripting vulnerability in its HTML Manager interface. A remote attacker can exploit this to inject code into a user's browser via a crafted URL. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Update Apache Tomcat to version 7.0.6 or later. | | |
| **Remark** | http://www.nessus.org/u?1b4b157f https://seclists.org/fulldisclosure/2011/Feb/78 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 35 | **Finding** | Apache Tomcat 6.0.32 / 7.0.8 NIO Connector DoS |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat listening on the remote host is prior to 6.0.32 or 7.0.8. It is, therefore, affected by a denial of service vulnerability. An error, involving the NIO HTTP connector, exists such that the limit 'maxHttpHeaderSize' is not enforced thereby allowing a denial of service condition when memory is exhausted. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Update Apache Tomcat to version 6.0.32 / 7.0.8 or later. | | |
| **Remark** | http://www.nessus.org/u?1fba1931 http://www.nessus.org/u?eacc755c http://www.nessus.org/u?daf049a2 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 36 | **Finding** | Apache Tomcat 7.x 7.0.11 @ServletSecurity Annotation Security Bypass |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.x listening on the remote host is prior to 7.0.11, It is, therefore affected by a security bypass vulnerability. When a web application is started, 'ServletSecurity' annotations might be ignored which could lead to some areas of the applications not being protected as expected. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.11 or later. | | |
| **Remark** | http://www.nessus.org/u?e95c3250 http://www.nessus.org/u?dfd5efff | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 37 | **Finding** | Apache Tomcat 7.x 7.0.12 Multiple Vulnerabilities |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.x listening on the remote host is prior to 7.0.12. It is, therefore, affected by multiple vulnerabilities :  - A fix for CVE-2011-1088 introduced a security bypass  vulnerability. If login configuration data is absent  from the 'web.xml' file and a web application is  marked as 'metadata-complete', security constraints are  ignored and may be bypassed by an attacker. Please note  this vulnerability only affects version 7.0.11 of  Tomcat. (CVE-2011-1183)  - Several weaknesses were found in the HTTP Digest  authentication implementation. The issues are as  follows: replay attacks are possible, server nonces  are not checked, client nonce counts are not checked,  'quality of protection' (qop) values are not checked,  realm values are not checked, and the server secret is  a hard-coded, known string. The effect of these issues  is that Digest authentication is no stronger than Basic  authentication. (CVE-2011-1184, CVE-2011-5062,  CVE-2011-5063, CVE-2011-5064)  - Updates to the HTTP BIO connector, in support of  Servlet 3.0 asynchronous requests, fail to completely  handle HTTP pipelining. Sensitive information may be  disclosed because responses from the server can be  improperly returned to the wrong request and possibly  to the wrong user. (CVE-2011-1475) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.12 or later. | | |
| **Remark** | http://www.nessus.org/u?343187a6 https://bz.apache.org/bugzilla/show\_bug.cgi?id=50928 http://svn.apache.org/viewvc?view=revision=1087643 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 38 | **Finding** | Apache Tomcat 7.0.12 / 7.0.13 Security Constraint Bypass |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.0.12 or 7.0.13 listening on the remote host is affected by a security constraint bypass vulnerability. Fixes for CVE-2011-1088 and CVE-2011-1183 introduced an error in 'core/StandardWrapper.java' which allows an incorrect class loader to be used. The effect of this is that security constraints configured through annotations are ignored on the initial request to a servlet. However, further requests are secured properly. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.14 or later. | | |
| **Remark** | http://www.nessus.org/u?1a1f0794 http://svn.apache.org/viewvc?view=revision=1100832 https://seclists.org/bugtraq/2011/May/134 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 39 | **Finding** | Apache Tomcat 7.x 7.0.17 Multiple Vulnerabilities |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.x listening on the remote host is prior to 7.0.17. It is, therefore, affected by the following vulnerabilities :  - An error handling issue exists related to the  MemoryUserDatabase that allows user passwords to be  disclosed through log files. (CVE-2011-2204)  - If loaded before other web applications, a malicious web  application can potentially access or modify the  web.xml, context.xml, and TLD files of other web  applications on the system. (CVE-2011-2481)  - An input validation error exists that allows a local  attacker to either bypass security or carry out denial  of service attacks when the APR or NIO connectors are  enabled. (CVE-2011-2526) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.19 or later. Note that versions 7.0.17 and 7.0.18 are not affected but were never officially released. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.19 https://www.mail-archive.com/announce@tomcat.apache.org/msg00053.html https://www.mail-archive.com/announce@tomcat.apache.org/msg00055.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 40 | **Finding** | Apache Tomcat 7.x 7.0.20 'jsvc' Information Disclosure |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.x listening on the remote host is prior to 7.0.20. It is, therefore, affected by an information disclosure vulnerability due to a component that Apache Tomcat relies on called 'jsvc' which does not drop capabilities after starting and can allow access to sensitive files owned by the super user. Note that this vulnerability only affects Linux operating systems and only when the following are true :  - jsvc is compiled with libpcap  - the '-user' parameter is used Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.20 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.20 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 41 | **Finding** | Apache Tomcat 7.x 7.0.22 Multiple Vulnerabilities |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.x listening on the remote host is prior to 7.0.22. It is, therefore, affected by multiple vulnerabilities :  - An information disclosure vulnerability exists. Request  information is cached in two objects, and these objects  are not recycled at the same time. Further requests can  obtain sensitive information if certain error conditions  occur. (CVE-2011-3375)  - The web server is not properly restricting access to  the servlets that provide the functionality of the  Manager application. This can allow untrusted web  applications to access privileged internal functionality  such as gathering information on running web  applications and deploying additional web applications.  (CVE-2011-3376) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.22 or later. | | |
| **Remark** | http://svn.apache.org/viewvc?view=revision=1176588 http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.22 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 42 | **Finding** | Apache Tomcat 7.x 7.0.23 Hash Collision DoS |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.x listening on the remote host is prior to 7.0.23. It is, therefore, affected by a denial of service vulnerability. Large numbers of crafted form parameters can cause excessive CPU consumption due to hash collisions. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.23 or later. Alternatively, as a workaround, set the 'maxPostSize' configuration variable to the lowest sensible value required to support your hosted applications. | | |
| **Remark** | http://www.nessus.org/u?d97dc97c http://www.nruns.com/\_downloads/advisory28122011.pdf http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.23 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 43 | **Finding** | Apache Tomcat 7.0.x 7.0.28 Multiple DoS |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.0 listening on the remote host is prior to 7.0.28. It is, therefore, affected by the following vulnerabilities :  - A flaw exists within the parseHeaders() function that  allows an attacker, via a crafted header, to cause a  remote denial of service. (CVE-2012-2733)  - An error exists related to the 'NIO' connector when  HTTPS and 'sendfile' are enabled that can force the  application into an infinite loop. (CVE-2012-4534) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.28 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.28 https://seclists.org/fulldisclosure/2012/Dec/72 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 44 | **Finding** | Apache Tomcat 7.0.x 7.0.30 Multiple Vulnerabilities |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.0 listening on the remote host is prior to 7.0.30. It is, therefore, affected by the following vulnerabilities :  - An error related to chunked transfer encoding and  extensions allows limited denial of service attacks.  (CVE-2012-3544)  - An error exists related to FORM authentication that  allows security bypass if 'j\_security\_check' is appended  to the request. (CVE-2012-3546)  - Replay-countermeasure functionality in HTTP Digest  Access Authentication tracks cnonce values instead of  nonce values, which makes it easier for attackers to  bypass access restrictions by sniffing the network for  valid requests. (CVE-2012-5885)  - HTTP Digest Access Authentication implementation caches  information about the authenticated user, which allows  an attacker to bypass authentication via session ID.  (CVE-2012-5886)  - HTTP Digest Access Authentication implementation does  not properly check for stale nonce values with  enforcement of proper credentials, which allows an  attacker to bypass restrictions by sniffing requests.  (CVE-2012-5887) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.30 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.30 https://seclists.org/fulldisclosure/2012/Dec/73 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 45 | **Finding** | Apache Tomcat 7.0.x 7.0.32 XSRF Filter Bypass |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.0 listening on the remote host is prior to 7.0.32. It is, therefore, affected by a security bypass vulnerability due to an error in the file 'filters/CsrfPreventionFilter.java' that allows cross-site request forgery (XSRF) attacks to bypass the filtering. This allows access to protected resources without a session identifier. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Update Apache Tomcat to version 7.0.32 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.32 https://seclists.org/fulldisclosure/2012/Dec/74 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 46 | **Finding** | Apache Tomcat 7.0.x 7.0.33 Session Fixation |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.0 listening on the remote host is prior to 7.0.33. It is, therefore, affected by an error related to HTML form authentication and session fixation that allows an attacker to carry out requests using a victim's credentials. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Update to Apache Tomcat version 7.0.33 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.33 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 47 | **Finding** | Apache Tomcat 7.0.x 7.0.40 Multiple Vulnerabilities |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.0 listening on the remote host is prior to 7.0.40. It is, therefore, affected by multiple vulnerabilities :    - An error exists related to 'AsyncListeners' that throw  'RuntimeExceptions' that allow elements of certain  requests to be disclosed in responses to other requests.  (CVE-2013-2071)  - It is possible to upload a malicious JSP to a Tomcat  server and subsequently trigger execution of that JSP.  (CVE-2013-4444) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Update to Apache Tomcat version 7.0.40 or later. | | |
| **Remark** | https://www.securityfocus.com/archive/1/533399/30/0/threaded http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.40 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 48 | **Finding** | Apache Tomcat 7.0.x 7.0.50 Multiple Vulnerabilities |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.0.x listening on the remote host is prior to 7.0.50. It is, therefore, affected by the following vulnerabilities :  - The fix for CVE-2012-3544 was not complete and limits  are not properly applied to chunk extensions and  whitespaces in certain trailing headers. This error  could allow denial of service attacks. (CVE-2013-4322)  - The application allows XML External Entity (XXE)  processing that could disclose sensitive information.  (CVE-2013-4590) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Update to Apache Tomcat version 7.0.50 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.50 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 49 | **Finding** | Apache Tomcat 7.0.x 7.0.53 Multiple Vulnerabilities |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.0.x listening on the remote host is prior to 7.0.53. It is, therefore, affected by the following vulnerabilities :  - An error exists related to chunk size and chunked  requests that allow denial of service attacks.  (CVE-2014-0075)  - An error exists related to XSLT handling and security  managers that allows security bypass related to external  XML entities. (CVE-2014-0096)  - An error exists related to content length header  handling and using the application behind a reverse  proxy that allows a security bypass. (CVE-2014-0099) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.53 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.53 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 50 | **Finding** | Apache Tomcat 7.0.x 7.0.54 XML Parser Information Disclosure |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the instance of Apache Tomcat 7.0.x listening on the remote host is prior to 7.0.54. It is, therefore, affected by an information disclosure vulnerability. An error exists that allows undesired XML parsers to be injected into the application by a malicious web application, allows the bypassing of security controls, and allows the processing of external XML entities. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.54 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.54 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 51 | **Finding** | Apache Tomcat 7.0.x 7.0.55 Multiple Vulnerabilities |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat service listening on the remote host is 7.0.x prior to 7.0.55. It is, therefore, affected by the following vulnerabilities :  - A race condition exists in the ssl3\_read\_bytes()  function when SSL\_MODE\_RELEASE\_BUFFERS is enabled. This  allows a remote attacker to inject data across sessions  or cause a denial of service. (CVE-2010-5298)  - A buffer overflow error exists related to invalid DTLS  fragment handling that can lead to the execution of  arbitrary code. Note that this issue only affects  OpenSSL when used as a DTLS client or server.  (CVE-2014-0195)  - An error exists in the do\_ssl3\_write() function that  allows a NULL pointer to be dereferenced, resulting in a  denial of service. Note that this issue is exploitable  only if 'SSL\_MODE\_RELEASE\_BUFFERS' is enabled.  (CVE-2014-0198)  - An error exists related to DTLS handshake handling that  can lead to denial of service attacks. Note that this  issue only affects OpenSSL when used as a DTLS client.  (CVE-2014-0221)  - An unspecified error exists in how ChangeCipherSpec  messages are processed that can allow an attacker to  cause usage of weak keying material, leading to  simplified man-in-the-middle attacks. (CVE-2014-0224)  - An error exists in 'ChunkedInputFilter.java' due to  improper handling of attempts to continue reading data  after an error has occurred. This allows a remote  attacker, via streaming data with malformed chunked  transfer coding, to conduct HTTP request smuggling or  cause a denial of service. (CVE-2014-0227)  - An error exists due to a failure to limit the size of  discarded requests. A remote attacker can exploit this  to exhaust available memory resources, resulting in a  denial of service condition. (CVE-2014-0230)  - An unspecified error exists related to anonymous ECDH  cipher suites that can allow denial of service attacks.  Note that this issue only affects OpenSSL TLS clients.  (CVE-2014-3470) Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.55 or later. | | |
| **Remark** | http://tomcat.apache.org/download-70.cgi#7.0.55 https://bz.apache.org/bugzilla/show\_bug.cgi?id=56596 https://www.openssl.org/news/secadv/20140605.txt | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 52 | **Finding** | Apache Tomcat 7.0.x 7.0.60 Multiple Vulnerabilities (FREAK) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat service listening on the remote host is 7.0.x prior to 7.0.60. It is, therefore, affected by the following vulnerabilities :  - A NULL pointer dereference flaw exists when the SSLv3  option isn't enabled and an SSLv3 ClientHello is  received. This allows a remote attacker, using an  unexpected handshake, to crash the daemon, resulting in  a denial of service. (CVE-2014-3569)  - The BIGNUM squaring (BN\_sqr) implementation does not  properly calculate the square of a BIGNUM value. This  allows remote attackers to defeat cryptographic  protection mechanisms. (CVE-2014-3570)  - A NULL pointer dereference flaw exists with  dtls1\_get\_record() when handling DTLS messages. A remote  attacker, using a specially crafted DTLS message, can  cause a denial of service. (CVE-2014-3571)  - A flaw exists with ECDH handshakes when using an ECDSA  certificate without a ServerKeyExchange message. This  allows a remote attacker to trigger a loss of forward  secrecy from the ciphersuite. (CVE-2014-3572)  - A flaw exists when accepting non-DER variations of  certificate signature algorithms and signature encodings  due to a lack of enforcement of matches between signed  and unsigned portions. A remote attacker, by including  crafted data within a certificate's unsigned portion,  can bypass fingerprint-based certificate-blacklist  protection mechanisms. (CVE-2014-8275)  - A security feature bypass vulnerability, known as FREAK  (Factoring attack on RSA-EXPORT Keys), exists due to the  support of weak EXPORT\_RSA cipher suites with keys less  than or equal to 512 bits. A man-in-the-middle attacker  may be able to downgrade the SSL/TLS connection to use  EXPORT\_RSA cipher suites which can be factored in a  short amount of time, allowing the attacker to intercept  and decrypt the traffic. (CVE-2015-0204)  - A flaw exists when accepting DH certificates for client  authentication without the CertificateVerify message.  This allows a remote attacker to authenticate to the  service without a private key. (CVE-2015-0205)  - A memory leak occurs in dtls1\_buffer\_record()  when handling a saturation of DTLS records containing  the same number sequence but for the next epoch. This  allows a remote attacker to cause a denial of service.  (CVE-2015-0206)  - A use-after-free condition exists in the  d2i\_ECPrivateKey() function due to improper processing  of malformed EC private key files during import. A  remote attacker can exploit this to dereference or free  already freed memory, resulting in a denial of service  or other unspecified impact. (CVE-2015-0209)  - An invalid read flaw exists in the ASN1\_TYPE\_cmp()  function due to improperly performed boolean-type  comparisons. A remote attacker can exploit this, via a  crafted X.509 certificate to an endpoint that uses the  certificate-verification feature, to cause an invalid  read operation, resulting in a denial of service.  (CVE-2015-0286)  - A flaw exists in the ASN1\_item\_ex\_d2i() function due to  a failure to reinitialize 'CHOICE' and 'ADB' data  structures when reusing a structure in ASN.1 parsing.  This allows a remote attacker to cause an invalid write  operation and memory corruption, resulting in a denial  of service. (CVE-2015-0287)  - A NULL pointer dereference flaw exists in the  X509\_to\_X509\_REQ() function due to improper processing  of certificate keys. This allows a remote attacker, via  a crafted X.509 certificate, to cause a denial of  service. (CVE-2015-0288)  - A NULL pointer dereference flaw exists in the PKCS#7  parsing code due to incorrect handling of missing outer  ContentInfo. This allows a remote attacker, using an  application that processes arbitrary PKCS#7 data and  providing malformed data with ASN.1 encoding, to cause  a denial of service. (CVE-2015-0289)  - A flaw exists in servers that both support SSLv2 and  enable export cipher suites due to improper  implementation of SSLv2. A remote attacker can exploit  this, via a crafted CLIENT-MASTER-KEY message, to cause  a denial of service. (CVE-2015-0293) Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.60 or later. | | |
| **Remark** | http://tomcat.apache.org/tomcat-7.0-doc/changelog.html https://www.openssl.org/news/openssl-1.0.1-notes.html https://www.openssl.org/news/secadv/20150108.txt https://www.openssl.org/news/vulnerabilities.html https://www.smacktls.com/#freak https://www.openssl.org/news/secadv/20150319.txt | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 53 | **Finding** | Apache Tomcat 7.0.x 7.0.59 Security Manager Bypass |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat server listening on the remote host is 7.0.x prior to 7.0.59. It is, therefore, affected by a security bypass vulnerability due to a flaw that occurs when handling expression language. A remote attacker can exploit this, via a crafted web application, to bypass the security manager protection and execute arbitrary code. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.59 or later. | | |
| **Remark** | http://www.nessus.org/u?edd653ec http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.59 https://seclists.org/bugtraq/2015/May/94 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 54 | **Finding** | Apache Tomcat 7.0.x 7.0.68 Multiple Vulnerabilities |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat service running on the remote host is 7.0.x prior to 7.0.68. It is, therefore, affected by multiple vulnerabilities :  - An information disclosure vulnerability exists due to  a failure to enforce access restrictions when handling  directory requests that are missing trailing slashes. An  unauthenticated, remote attacker can exploit this to  enumerate valid directories. (CVE-2015-5345)  - An information disclosure vulnerability exists in the  Manager and Host Manager web applications due to a flaw  in the index page when issuing redirects in response to  unauthenticated requests for the root directory of the  application. An unauthenticated, remote attacker can  exploit this to gain access to the XSRF token  information stored in the index page. Note that the  Apache Tomcat advisory does not list Tomcat version  7.0.0 as affected by this vulnerability. (CVE-2015-5351)  - An information disclosure vulnerability exists that  allows a specially crafted web application to load the  StatusManagerServlet. An attacker can exploit this to  gain unauthorized access to a list of all deployed  applications and a list of the HTTP request lines for  all requests currently being processed. (CVE-2016-0706)  - A security bypass vulnerability exists due to a flaw  in the StandardManager, PersistentManager, and cluster  implementations that is triggered when handling  persistent sessions. An unauthenticated, remote attacker  can exploit this, via a crafted object in a session, to  bypass the security manager and execute arbitrary code.  (CVE-2016-0714)  - A flaw exists due to the setGlobalContext() method of  ResourceLinkFactory being accessible to web applications  even when run under a security manager. An  unauthenticated, remote attacker can exploit this to  inject malicious global context, allowing data owned by  other web applications to be read or written to.  (CVE-2016-0763) Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.68 or later. | | |
| **Remark** | http://www.nessus.org/u?40843ffb | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 55 | **Finding** | Apache Tomcat 6.0.x 6.0.47 / 7.0.x 7.0.72 / 8.0.x 8.0.37 / 8.5.x 8.5.5 / 9.0.x 9.0.0.M10 Multiple Vulnerabilities |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat service running on the remote host is 6.0.x prior to 6.0.47, 7.0.x prior to 7.0.72, 8.0.x prior to 8.0.37, 8.5.x prior to 8.5.5 or 9.0.x prior to 9.0.0.M10. It is, therefore, affected by multiple  vulnerabilities :  - An information disclosure vulnerability exists due to a  failure to process passwords when paired with a  non-existent username. An unauthenticated, remote  attacker can exploit this, via a timing attack, to  enumerate user account names. (CVE-2016-0762)  - A security bypass vulnerability exists that allows a  local attacker to bypass a configured SecurityManager  via a utility method that is accessible to web  applications. (CVE-2016-5018)  - An information disclosure vulnerability exists in the  SecurityManager component due to a failure to properly  restrict access to system properties for the  configuration files system property replacement feature.  An attacker can exploit this, via a specially crafted  web application, to bypass SecurityManager restrictions  and disclose system properties. (CVE-2016-6794)  - A security bypass vulnerability exists that allows a  local attacker to bypass a configured SecurityManager by  changing the configuration parameters for a JSP servlet.  (CVE-2016-6796)  - A security bypass vulnerability exists due to a failure  to limit web application access to global JNDI  resources. A local attacker can exploit this to gain  unauthorized access to resources. (CVE-2016-6797) Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 6.0.47 / 7.0.72 / 8.0.37 / 8.5.5 / 9.0.0.M10 or later. Note that versions 6.0.46 and 7.0.71 also resolve the vulnerabilities; however, these versions were never officially released by the vendor. | | |
| **Remark** | http://www.nessus.org/u?5c3fa418 http://www.nessus.org/u?be50738a http://www.nessus.org/u?47795ca8 http://www.nessus.org/u?afe6a582 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 56 | **Finding** | Apache Tomcat 6.0.16 6.0.50 / 7.0.x 7.0.75 / 8.0.x 8.0.41 / 8.5.x 8.5.9 / 9.0.x 9.0.0.M15 NIO HTTP Connector Information Disclosure |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat service running on the remote host is 6.0.16 prior to 6.0.50, 7.0.x prior to 7.0.75, 8.0.x prior to 8.0.41, 8.5.x prior to 8.5.9, or  9.0.x prior to 9.0.0.M15. It is therefore, affected by an information  disclosure vulnerability in error handling during send file processing  by the NIO HTTP connector, in which an error can cause the current  Processor object to be added to the Processor cache multiple times.  This allows the same Processor to be used for concurrent requests.  An unauthenticated, remote attacker can exploit this issue, via a  shared Processor, to disclose sensitive information, such as session  IDs, response bodies related to another request, etc. Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 6.0.50 / 7.0.75 / 8.0.41 / 8.5.9 /  9.0.0.M15 or later. For the 6.0.x version branch, the vulnerability  was fixed in 6.0.49; however, that release candidate was not approved,  and 6.0.50 is still pending release. | | |
| **Remark** | http://www.nessus.org/u?3a06fd01 https://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.5.9 http://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.0.41 http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.75 http://tomcat.apache.org/security-6.html#Fixed\_in\_Apache\_Tomcat\_6.0.50 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 57 | **Finding** | Apache Tomcat 6.0.x 6.0.53 / 7.0.x 7.0.77 / 8.0.x 8.0.43 Pipelined Requests Information Disclosure |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat service running on the remote host is 6.0.x prior to 6.0.53, 7.0.x prior to 7.0.77, or 8.0.x prior to 8.0.43. It is therefore, affected by a flaw in the handling of pipelined requests when send file processing is used that results in the pipelined request being lost when processing of the previous request has completed, causing responses to be sent for the wrong request. An unauthenticated, remote attacker can exploit this to disclose sensitive information. Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 6.0.53 / 7.0.77 / 8.0.43 or later. | | |
| **Remark** | https://tomcat.apache.org/security-6.html#Fixed\_in\_Apache\_Tomcat\_6.0.53 https://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.77 https://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.0.43 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 58 | **Finding** | Apache Tomcat 7.0.x 7.0.78 / 8.0.x 8.0.44 / 8.5.x 8.5.15 / 9.0.x 9.0.0.M21 Remote Error Page Manipulation |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat service running on the remote host is 7.0.x prior to 7.0.78, 8.0.x prior to 8.0.44, 8.5.x prior to 8.5.15, or 9.0.x prior to 9.0.0.M21. It is, therefore, affected by an implementation flaw in the error  page reporting mechanism in which it does not conform to the Java  Servlet Specification that requires static error pages to be processed  as an HTTP GET request nothwithstanding the HTTP request method that  was originally used when the error occurred. Depending on the original  request and the configuration of the Default Servlet, an  unauthenticated, remote attacker can exploit this issue to replace or  remove custom error pages. Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.78 / 8.0.44 / 8.5.15 / 9.0.0.M21 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.78 http://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.0.44 http://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.5.15 http://www.nessus.org/u?a774a43b | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 59 | **Finding** | Apache Tomcat 7.0.x 7.0.81 Multiple Vulnerabilities |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 7.0.x prior to 7.0.81. It is, therefore, affected by multiple vulnerabilities :  - An unspecified vulnerability when running on Windows  with HTTP PUTs enabled (e.g. via setting the readonly  initialization parameter of the Default to false) makes  it possible to upload a JSP file to the server via a  specially crafted request. This JSP could then be  requested and any code it contained would be  executed by the server. (CVE-2017-12615, CVE-2017-12617)  - When using a VirtualDirContext it was possible to bypass  security constraints and/or view the source code of JSPs  for resources served by the VirtualDirContext using a  specially crafted request. (CVE-2017-12616) Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.81 or later. Note that the remote code execution issue was fixed in Apache Tomcat 7.0.80 but the release vote for the 7.0.81 release candidate did not pass. Therefore, although users must download 7.0.81 to obtain a version that includes the fix for this issue, version 7.0.80 is not included in the list of affected versions. | | |
| **Remark** | http://www.nessus.org/u?d6b65377 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 60 | **Finding** | Apache Tomcat 7.0.x 7.0.82 / 8.5.x 8.5.23 Multiple Vulnerabilities |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 7.0.x prior to 7.0.82 or 8.5.x prior to 8.5.23. It is, therefore, affected by an unspecified vulnerability when running with HTTP PUTs enabled (e.g. via setting the readonly initialization parameter of the Default to false) that makes it possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server. Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.82 / 8.5.23 or later. | | |
| **Remark** | http://www.nessus.org/u?4f047e41 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 61 | **Finding** | Apache Tomcat 7.0.x 7.0.82 Multiple Vulnerabilities |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 7.0.x prior to 7.0.82. It is, therefore, affected by an unspecified vulnerability when running on Windows with HTTP PUTs enabled (e.g. via setting the readonly initialization parameter of the Default to false) makes it possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server. Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.82 or later. | | |
| **Remark** | http://www.nessus.org/u?bbdfd5cb | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 62 | **Finding** | Apache Tomcat 7.0.0 7.0.85 Security Constraint Weakness |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 7.0.x prior to 7.0.85. It is, therefore, affected by a security constraints flaw which could expose resources to unauthorized users. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.85 or later. | | |
| **Remark** | http://www.nessus.org/u?170a880f | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 63 | **Finding** | Apache Tomcat 8.5.x 8.5.34 Open Redirect Weakness |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 8.5.x prior to 8.5.34. It is, therefore, affected by a open redirect  vulnerability. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.34 or later. | | |
| **Remark** | http://www.nessus.org/u?1bddf0bb | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 64 | **Finding** | Apache Tomcat 7.0.2 Denial of Service and Information Disclosure |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat instance listening on the remote host is prior to 7.0.2. It is, therefore, affected by a denial of service vulnerability which could also lead to information disclosure. A remote attacker could trigger flaws in the handling of the Transfer-Encoding header to cause a denial of service or potentially leak information. Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.2 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.2 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 65 | **Finding** | Apache Tomcat 7.0.x 7.0.47 / 8.0.x 8.0.0-RC3 Information Disclosure |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat instance listening on the remote host is 7.0.x prior to 7.0.47 or  8.0.x prior to 8.0.0-RC3. It is, therefore, affected by the following  vulnerability:    - An information disclosure vulnerability exists in Tomcat due to   improper handling of content-length headers. An unauthenticated,   remote attacker can exploit this to disclose potentially sensitive   information. Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.47 / 8.0.0-RC3 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.47 http://www.nessus.org/u?4209777a | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 66 | **Finding** | Apache Tomcat 7.0.x 7.0.65 / 8.0.x 8.0.27 Directory Traversal |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat instance listening on the remote host is 7.0.x prior to 7.0.65, or 8.0.x prior to 8.0.27. It is, therefore, affected by the following  vulnerability:    - A directory traversal vulnerability exists in Tomcat when   accessing resources via ServletContext methods using paths  beginning with '/..'. An unauthenticated, remote attacker can   exploit this, by sending a specially crafted request, to   obtain a directory listing for the directory in which the  application was deployed.  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.65 / 8.0.27 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.65 http://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.0.27 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 67 | **Finding** | Apache Tomcat 7.0.67 Session Fixation |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat instance listening on the remote host is prior to 7.0.67. It is, therefore, affected by a session fixation vulnerability:  - A flaw exists due to a failure to invalidate a previous  session ID when assigning an ID to a new session. An  attacker can exploit this, via a crafted request that  uses the requestedSessionSSL field to fixate the session  ID, to ensure that the user authenticates with a known  session ID, allowing the session to be subsequently  hijacked. Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.67 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.67 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 68 | **Finding** | Apache Tomcat 7.0.x 7.0.76 / 8.0.x 8.0.42 / 8.5.x 8.5.12 / 9.0.x 9.0.0.M18 Improper Access Control |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat instance listening on the remote host is 7.0.x prior to 7.0.76, 8.0.x 8.0.42, 8.5.x 8.5.12 or 9.0.x 9.0.0.M18. It is, therefore, affected by the following vulnerability:  - An improper access control vulnerability exists when  calls to application listeners do not use the appropriate  facade object. This allows untrusted applications to  potentially access and modify information associated  with other web applications.  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.76 / 8.0.42 / 8.5.12 / 9.0.0.M18 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.76 http://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.0.42 http://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.5.12 http://www.nessus.org/u?3f871212 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 69 | **Finding** | Apache Tomcat 8.5.0 8.5.41 DoS |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.41. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_8.5.41\_security-8 advisory.  - The fix for CVE-2019-0199 was incomplete and did not  address HTTP/2 connection window exhaustion on write. By  not sending WINDOW\_UPDATE messages for the connection  window (stream 0) clients were able to cause server-side  threads to block eventually leading to thread exhaustion  and a DoS. (CVE-2019-10072) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.41 or later. | | |
| **Remark** | https://github.com/apache/tomcat/commit/0bcd69c https://github.com/apache/tomcat/commit/8d14c6f https://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.5.41 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 70 | **Finding** | Apache Tomcat 8.5.0 8.5.49 Privilege Escalation |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.49. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_8.5.49\_security-8 advisory.  - When Apache Tomcat is configured with the JMX Remote   Lifecycle Listener, a local attacker without access to   the Tomcat process or configuration files is able to   manipulate the RMI registry to perform a man-in-the-middle   attack to capture user names and passwords used to access   the JMX interface. The attacker can then use these   credentials to access the JMX interface and gain complete   control over the Tomcat instance. (CVE-2019-12418) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.49 or later. | | |
| **Remark** | https://github.com/apache/tomcat/commit/a91d7db http://www.nessus.org/u?ed6582f2 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 71 | **Finding** | Apache Tomcat 8.5.0 8.5.50 Privilege Escalation Vulnerability |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.50. It is, therefore, affected by a privilege escalation vulnerability as referenced in the 'Fixed in Apache Tomcat 8.5.50' advisory.  - When using FORM authentication there was a narrow window where an attacker could perform a session  fixation attack. The window was considered too narrow for an exploit to be practical but, erring on the  side of caution, this issue has been treated as a security vulnerability. (CVE-2019-17563) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.50 or later. | | |
| **Remark** | https://github.com/apache/tomcat/commit/e19a202 http://www.nessus.org/u?e0b173ef | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 72 | **Finding** | nginx 1.17.7 Information Disclosure |
| **Severity** | **Medium** | **Port** | TCP: 80, 443 |
| **Target** | 172.28.130.190(80, 443) | | |
| **Detail** | According to its Server response header, the installed version of nginx is prior to 1.17.7. It is, therefore, affected by an information disclosure vulnerability. | | |
| **Solution** | Upgrade to nginx version 1.17.7 or later. | | |
| **Remark** | http://www.nessus.org/u?fd026623 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 73 | **Finding** | Apache Tomcat 7.0.0 7.0.104 Remote Code Execution |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 7.0.104. It is, therefore, affected by a remote code execution vulnerability as referenced in the fixed\_in\_apache\_tomcat\_7.0.104\_security-7 advisory. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.104 or later. | | |
| **Remark** | http://www.nessus.org/u?d383947b | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 74 | **Finding** | Apache Tomcat 8.5.x 8.5.55 Remote Code Execution |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.x prior to 8.5.55. It is, therefore, affected by a  remote code execution vulnerability as referenced in the fixed\_in\_apache\_tomcat\_8.5.55\_security-8 advisory.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version  number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.55 or later. | | |
| **Remark** | http://www.nessus.org/u?9502c510 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 75 | **Finding** | Apache Tomcat 8.5.0 8.5.56 DoS |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.56. It is, therefore, affected by a denial of service vulnerability as referenced in the fixed\_in\_apache\_tomcat\_8.5.56\_security-8 advisory. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.56 or later. | | |
| **Remark** | http://www.nessus.org/u?9a501720 http://www.nessus.org/u?0ff2bf8c | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 76 | **Finding** | Apache Tomcat 8.5.0 8.5.57 Multiple Vulnerabilities |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | The version of Tomcat installed on the remote host is 8.5.x prior to 8.5.57. It is, therefore, affected by multiple vulnerabilities as referenced in the Fixed in Apache Tomcat 8.5.57 security advisory.  - The payload length in a WebSocket frame was not correctly validated. Invalid payload lengths could trigger  an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service (DoS).  (CVE-2020-13935)  - An h2c direct connection did not release the HTTP/1.1 processor after the upgrade to HTTP/2. If a  sufficient number of such requests were made, an OutOfMemoryException could occur leading to a denial of  service (DoS). (CVE-2020-13934) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.57 or later. | | |
| **Remark** | http://www.nessus.org/u?cd59de72 http://www.nessus.org/u?7358785a http://www.nessus.org/u?78f0e4ba | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 77 | **Finding** | Apache Tomcat 8.5.x 8.5.58 / 9.0.x 9.0.38 HTTP/2 Request Mix-Up |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | The version of Tomcat installed on the remote host is 8.5.x prior to 8.5.58 or 9.0.x prior to 9.0.38. It is, therefore, affected by a vulnerability. If an HTTP/2 client exceeds the agreed maximum number of concurrent streams for a connection (in violation of the HTTP/2 protocol), it is possible that a subsequent request made on that connection could contain HTTP headers - including HTTP/2 pseudo headers - from a previous request rather than the intended headers. This can lead to users seeing responses for unexpected resources. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.58, 9.0.38 or later. | | |
| **Remark** | http://www.nessus.org/u?0656cf04 http://www.nessus.org/u?771617a1 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 78 | **Finding** | Apache Tomcat 8.5.x 8.5.60 Information Disclosure |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.60. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed\_in\_apache\_tomcat\_8.5.60\_security-8 advisory.  - When serving resources from a network location using the NTFS file system, Apache Tomcat versions  10.0.0-M1 to 10.0.0-M9, 9.0.0.M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP  source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE API  File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API  (FindFirstFileW) in some circumstances. (CVE-2021-24122)  - While investigating bug 64830 it was discovered that Apache Tomcat 10.0.0-M1 to 10.0.0-M9, 9.0.0-M1 to  9.0.39 and 8.5.0 to 8.5.59 could re-use an HTTP request header value from the previous stream received on  an HTTP/2 connection for the request associated with the subsequent stream. While this would most likely  lead to an error and the closure of the HTTP/2 connection, it is possible that information could leak  between requests. (CVE-2020-17527) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.60 or later. | | |
| **Remark** | http://www.nessus.org/u?05c4b1e2 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 79 | **Finding** | Apache Tomcat 8.5.0 8.5.63 Multiple Vulnerabilities |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.63. It is, therefore, affected by multiple vulnerabilities as referenced in the vendor advisory.  - When responding to new h2c connection requests, Apache Tomcat versions 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41   and 8.5.0 to 8.5.61 could duplicate request headers and a limited amount of request body from one request to   another meaning user A and user B could both see the results of user A's request. (CVE-2021-25122)  - When using Apache Tomcat 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41, 8.5.0 to 8.5.61 or 7.0.0. to 7.0.107 with a   configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to   CVE-2020-9494. Note that both the previously published prerequisites for CVE-2020-9484 and the previously   published mitigations for CVE-2020-9484 also apply to this issue. (CVE-2021-25329) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.63 or later. | | |
| **Remark** | http://www.nessus.org/u?b6278e74 http://www.nessus.org/u?0be223a3 http://www.nessus.org/u?15b6baad | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 80 | **Finding** | Apache Tomcat 7.0.0 7.0.108 RCE |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The fix for CVE-2020-9484 was incomplete. The version of Tomcat installed on the remote host is prior to 7.0.108.  It is, therefore, affected by a remote code execution vulnerability via deserialization. An attacker is able to control the contents and  name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and  c) the PersistenceManager is configured with sessionAttributeValueClassNameFilter=null (the default unless a  SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized; and  d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has  control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution  via deserialization of the file under their control. Note that both the previously published prerequisites for  CVE-2020-9484 and the previously published mitigations for CVE-2020-9484 also apply to this issue. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.108 or later. | | |
| **Remark** | http://www.nessus.org/u?e5b3746f http://www.nessus.org/u?b7d039d2 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 81 | **Finding** | Apache Tomcat 7.0.0 7.0.107 Information Disclosure |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 7.0.107. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_7.0.107\_security-7 advisory.  - When serving resources from a network location using the NTFS file system, Apache Tomcat versions  10.0.0-M1 to 10.0.0-M9, 9.0.0.M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP  source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE API  File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API  (FindFirstFileW) in some circumstances. (CVE-2021-24122) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.107 or later. | | |
| **Remark** | http://www.nessus.org/u?f528c7ca http://www.nessus.org/u?3e377be0 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 82 | **Finding** | Apache Tomcat 7.0.x = 7.0.108 / 8.5.x = 8.5.65 / 9.0.x = 9.0.45 / 10.0.x = 10.0.5 vulnerability |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8081, 8443, 8444 |
| **Target** | 172.28.130.190(443, 8080, 8081, 8443, 8444) | | |
| **Detail** | The version of Tomcat installed on the remote host is 7.0.x = 7.0.108 / 8.5.x = 8.5.65 / 9.0.x = 9.0.45 / 10.0.x =  10.0.5. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_10.0.6\_security-10  advisory.  - Queries made by the JNDI Realm did not always correctly escape parameters. Parameter values could be  sourced from user provided data (eg user names) as well as configuration data provided by an  administrator. In limited circumstances it was possible for users to authenticate using variations of  their user name and/or to bypass some of the protection provided by the LockOut Realm. (CVE-2021-30640) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.109, 8.5.66, 9.0.46, 10.0.6 or later. | | |
| **Remark** | http://www.nessus.org/u?d3fb2d8e http://www.nessus.org/u?0fb6f5ab http://www.nessus.org/u?0d761c19 http://www.nessus.org/u?ddfa2b5e http://www.nessus.org/u?95156892 http://www.nessus.org/u?ed08487c http://www.nessus.org/u?806274b5 http://www.nessus.org/u?f104a57d https://bz.apache.org/bugzilla/show\_bug.cgi?id=65224 http://www.nessus.org/u?837a9443 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 83 | **Finding** | Apache Tomcat 8.5.0 8.5.68 vulnerability |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.68. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_8.5.68\_security-8 advisory.  - Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP  transfer-encoding request header in some circumstances leading to the possibility to request smuggling  when used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if  the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding;  and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.  (CVE-2021-33037) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.68 or later. | | |
| **Remark** | http://www.nessus.org/u?ca148f18 http://www.nessus.org/u?9e0e6b06 http://www.nessus.org/u?bea8fba1 http://www.nessus.org/u?836aea5f | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 84 | **Finding** | Security Updates for Exchange (November 2021) (Remote) |
| **Severity** | **Medium** | **Port** | TCP: 444 |
| **Target** | 172.28.130.35(444), 172.28.130.37(444) | | |
| **Detail** | The Microsoft Exchange Server installed on the remote host is missing security updates. It is, therefore, affected by multiple vulnerabilities:  - A session spoofing vulnerability exists. An attacker can  exploit this to perform actions with the privileges of  another user. (CVE-2021-41349, CVE-2021-42305)  - A remote code execution vulnerability. An attacker can  exploit this to bypass authentication and execute  unauthorized arbitrary commands. (CVE-2021-42321) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Microsoft has released KB5007409 to address this issue. | | |
| **Remark** | https://support.microsoft.com/en-us/help/5007409 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 85 | **Finding** | JQuery 1.2 3.5.0 Multiple XSS |
| **Severity** | **Medium** | **Port** | TCP: 443, 8000, 8090 |
| **Target** | 172.28.131.24(8090), 172.28.135.188(8000), 172.28.140.45(443) | | |
| **Detail** | According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.  Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios  required for successful exploitation do not exist on devices running a PAN-OS release. | | |
| **Solution** | Upgrade to JQuery version 3.5.0 or later. | | |
| **Remark** | https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://security.paloaltonetworks.com/PAN-SA-2020-0007 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 86 | **Finding** | SMB Signing not required |
| **Severity** | **Medium** | **Port** | TCP: 445 |
| **Target** | 172.28.131.48(445), 172.28.131.108(445), 172.28.135.189(445), 172.28.135.223(445), 172.28.136.111(445), 172.28.136.153(445), 172.28.190.131(445), 172.28.190.133(445) | | |
| **Detail** | Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. | | |
| **Solution** | Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. | | |
| **Remark** | http://www.nessus.org/u?df39b8b3 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html http://www.nessus.org/u?a3cac4ea | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 87 | **Finding** | SSH Weak Algorithms Supported |
| **Severity** | **Medium** | **Port** | TCP: 22 |
| **Target** | 172.28.188.167(22), 172.28.188.168(22) | | |
| **Detail** | Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys. | | |
| **Solution** | Contact the vendor or consult product documentation to remove the weak ciphers. | | |
| **Remark** | https://tools.ietf.org/html/rfc4253#section-6.3 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 88 | **Finding** | Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness |
| **Severity** | **Medium** | **Port** | TCP: 3389 |
| **Target** | 172.28.131.108(3389), 172.28.135.223(3389), 172.28.136.111(3389), 172.28.137.112(3389), 172.28.190.131(3389), 172.28.190.139(3389) | | |
| **Detail** | The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP  client makes no effort to validate the identity of the server when  setting up encryption. An attacker with the ability to intercept  traffic from the RDP server can establish encryption with the client  and server without being detected. A MiTM attack of this nature would  allow the attacker to obtain any sensitive information transmitted,  including authentication credentials.  This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack. | | |
| **Solution** | - Force the use of SSL as a transport layer for this service if supported, or/and  - Select the 'Allow connections only from computers running Remote  Desktop with Network Level Authentication' setting if it is available. | | |
| **Remark** | http://www.nessus.org/u?8033da0d http://technet.microsoft.com/en-us/library/cc782610.aspx | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 89 | **Finding** | Terminal Services Encryption Level is Medium or Low |
| **Severity** | **Medium** | **Port** | TCP: 3389 |
| **Target** | 172.28.131.108(3389), 172.28.135.223(3389), 172.28.136.111(3389), 172.28.190.131(3389), 172.28.190.139(3389) | | |
| **Detail** | The remote Terminal Services service is not configured to use strong cryptography.  Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes. | | |
| **Solution** | Change RDP encryption level to one of :  3. High  4. FIPS Compliant | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 90 | **Finding** | Terminal Services Doesn't Use Network Level Authentication (NLA) Only |
| **Severity** | **Medium** | **Port** | TCP: 3389 |
| **Target** | 172.28.131.102(3389), 172.28.131.108(3389), 172.28.135.223(3389), 172.28.136.111(3389), 172.28.190.131(3389), 172.28.190.139(3389) | | |
| **Detail** | The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication,  NLA also helps protect the remote computer from malicious users and  software by completing user authentication before a full RDP  connection is established. | | |
| **Solution** | Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows. | | |
| **Remark** | https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11) http://www.nessus.org/u?e2628096 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 91 | **Finding** | AMQP Cleartext Authentication |
| **Severity** | **Medium** | **Port** | TCP: 5672 |
| **Target** | 172.28.131.102(5672) | | |
| **Detail** | The remote Advanced Message Queuing Protocol (AMQP) service supports one or more authentication mechanisms that allow credentials to be sent in the clear. | | |
| **Solution** | Disable cleartext authentication mechanisms in the AMQP configuration. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 92 | **Finding** | ESXi 6.5 / 6.7 XSS (VMSA-2020-0008) |
| **Severity** | **Medium** | **Port** | TCP: 443 |
| **Target** | 172.28.131.23(443), 172.28.140.41(443) | | |
| **Detail** | The remote VMware ESXi host is version 6.5 or 6.7 and is affected by a cross-site scripting (XSS) vulnerability in virtual machine attributes due to improper validation of user-supplied input before returning it to users. An authenticated, remote attacker with access to modify the system properties of a virtual machine from inside the guest OS can exploit this, by inserting script-related HTML in the system properties and having a user view the system properties from the ESXi Host Client, to execute arbitrary script code in a user's ESXi Host Client session. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2020-0008.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 93 | **Finding** | ESXi 6.5 / 6.7 / 7.0 DoS (VMSA-2020-0018) |
| **Severity** | **Medium** | **Port** | TCP: 443 |
| **Target** | 172.28.131.23(443), 172.28.140.41(443) | | |
| **Detail** | The remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by a denial of service (DoS) vulnerability in the authentication service. An unauthenticated, remote attacker can exploit this issue to exhaust memory resources  resulting in a degradation of performance condition while the attack is sustained. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2020-0018.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 94 | **Finding** | ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0004) |
| **Severity** | **Medium** | **Port** | TCP: 443 |
| **Target** | 172.28.131.23(443), 172.28.140.41(443) | | |
| **Detail** | The remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by multiple vulnerabilities, including the following:  - VMware ESXi, Workstation, and Fusion contain a use-after-free vulnerability in the XHCI USB controller. A  malicious actor with local administrative privileges on a virtual machine may exploit this issue to  execute code as the virtual machine's VMX process running on the host. (CVE-2021-22040)  - VMware ESXi, Workstation, and Fusion contain a double-fetch vulnerability in the UHCI USB controller. A  malicious actor with local administrative privileges on a virtual machine may exploit this issue to  execute code as the virtual machine's VMX process running on the host. (CVE-2021-22041)  - VMware ESXi contains an unauthorized access vulnerability due to VMX having access to settingsd  authorization tickets. A malicious actor with privileges within the VMX process only, may be able to  access settingsd service running as a high privileged user. (CVE-2021-22042) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2022-0004.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 95 | **Finding** | SSL Weak Cipher Suites Supported |
| **Severity** | **Medium** | **Port** | TCP: 3031 |
| **Target** | 172.28.131.24(3031) | | |
| **Detail** | The remote host supports the use of SSL ciphers that offer weak encryption. Note: This is considerably easier to exploit if the attacker is on the same physical network. | | |
| **Solution** | Reconfigure the affected application, if possible to avoid the use of weak ciphers. | | |
| **Remark** | http://www.nessus.org/u?6527892d | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 96 | **Finding** | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |
| **Severity** | **Medium** | **Port** | TCP: 3031 |
| **Target** | 172.28.131.24(3031) | | |
| **Detail** | The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections. As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service. The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism. This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability. | | |
| **Solution** | Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled. | | |
| **Remark** | https://www.imperialviolet.org/2014/10/14/poodle.html https://www.openssl.org/~bodo/ssl-poodle.pdf https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 97 | **Finding** | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) |
| **Severity** | **Medium** | **Port** | TCP: 3031 |
| **Target** | 172.28.131.24(3031) | | |
| **Detail** | The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key. | | |
| **Solution** | Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections. | | |
| **Remark** | https://drownattack.com/ https://drownattack.com/drown-attack-paper.pdf | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 98 | **Finding** | SMTP Server Non-standard Port Detection |
| **Severity** | **Medium** | **Port** | TCP: 25000 |
| **Target** | 172.28.137.52(25000) | | |
| **Detail** | This SMTP server is running on a non-standard port. This might be a backdoor set up by attackers to send spam or even control of a targeted machine. | | |
| **Solution** | Check and clean the configuration. | | |
| **Remark** | http://www.icir.org/vern/papers/backdoor/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 99 | **Finding** | ESXi 5.5 / 6.0 / 6.5 / 6.7 Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020) (remote check) |
| **Severity** | **Medium** | **Port** | TCP: 443 |
| **Target** | 172.28.140.41(443) | | |
| **Detail** | The remote VMware ESXi host is version 5.5, 6.0, 6.5, or 6.7 and is missing a security patch. It is, therefore, vulnerable to a speculative execution side channel attack known as L1 Terminal Fault (L1TF). An attacker who successfully exploited L1TF may be able to read privileged data across trust boundaries. | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2018-0020.html https://foreshadowattack.eu/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 100 | **Finding** | SSL Certificate Chain Contains RSA Keys Less Than 2048 bits |
| **Severity** | **Low** | **Port** | TCP: 443, 1433, 3031, 8443, 9090 |
| **Target** | 172.28.130.190(8443), 172.28.131.24(443, 3031, 9090), 172.28.135.189(1433) | | |
| **Detail** | At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits. Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014. Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt. | | |
| **Solution** | Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate. | | |
| **Remark** | https://www.cabforum.org/wp-content/uploads/Baseline\_Requirements\_V1.pdf | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 101 | **Finding** | SSL/TLS Diffie-Hellman Modulus = 1024 Bits (Logjam) |
| **Severity** | **Low** | **Port** | TCP: 8443, 10102 |
| **Target** | 172.28.130.190(8443), 172.28.131.49(10102) | | |
| **Detail** | The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections. | | |
| **Solution** | Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater. | | |
| **Remark** | https://weakdh.org/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 102 | **Finding** | SSH Server CBC Mode Ciphers Enabled |
| **Severity** | **Low** | **Port** | TCP: 22 |
| **Target** | 172.28.131.23(22), 172.28.131.24(22), 172.28.188.167(22), 172.28.188.168(22) | | |
| **Detail** | The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.  Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions. | | |
| **Solution** | Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 103 | **Finding** | SSH Weak MAC Algorithms Enabled |
| **Severity** | **Low** | **Port** | TCP: 22 |
| **Target** | 172.28.188.167(22), 172.28.188.168(22) | | |
| **Detail** | The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.  Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions. | | |
| **Solution** | Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 104 | **Finding** | SSH Weak Key Exchange Algorithms Enabled |
| **Severity** | **Low** | **Port** | TCP: 22 |
| **Target** | 172.28.188.167(22), 172.28.188.168(22) | | |
| **Detail** | The remote SSH server is configured to allow key exchange algorithms which are considered weak.  This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:   diffie-hellman-group-exchange-sha1   diffie-hellman-group1-sha1   gss-gex-sha1-\*   gss-group1-sha1-\*   gss-group14-sha1-\*   rsa1024-sha1  Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions. | | |
| **Solution** | Contact the vendor or consult product documentation to disable the weak algorithms. | | |
| **Remark** | http://www.nessus.org/u?b02d91cd https://datatracker.ietf.org/doc/html/rfc8732 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 105 | **Finding** | Terminal Services Encryption Level is not FIPS-140 Compliant |
| **Severity** | **Low** | **Port** | TCP: 3389 |
| **Target** | 172.28.131.108(3389), 172.28.135.223(3389), 172.28.136.111(3389), 172.28.190.131(3389), 172.28.190.139(3389) | | |
| **Detail** | The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant. | | |
| **Solution** | Change RDP encryption level to :  4. FIPS Compliant | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 106 | **Finding** | SSL Anonymous Cipher Suites Supported |
| **Severity** | **Low** | **Port** | TCP: 6001, 6101 |
| **Target** | 172.28.131.102(6001, 6101) | | |
| **Detail** | The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack. Note: This is considerably easier to exploit if the attacker is on the same physical network. | | |
| **Solution** | Reconfigure the affected application if possible to avoid use of weak ciphers. | | |
| **Remark** | http://www.nessus.org/u?3a040ada | | |



# 6 Port Discovery

| **Port** | **Protocol** | **Service** |
| --- | --- | --- |
| 21 | tcp | ftp |
| 22 | tcp | ssh |
| 25 | tcp | smtp |
| 53 | tcp | domain |
| 80 | tcp | http |
| 81 | tcp | hosts2-ns |
| 88 | tcp | kerberos-sec |
| 111 | tcp | rpcbind |
| 135 | tcp | msrpc |
| 139 | tcp | netbios-ssn |
| 389 | tcp | ldap |
| 427 | tcp | svrloc |
| 443 | tcp | https |
| 444 | tcp | snpp |
| 445 | tcp | microsoft-ds |
| 464 | tcp | kpasswd5 |
| 465 | tcp | smtps |
| 587 | tcp | submission |
| 593 | tcp | http-rpc-epmap |
| 636 | tcp | ldapssl |
| 808 | tcp | ccproxy-http |
| 902 | tcp | iss-realsecure |
| 1007 | tcp | unknown |
| 1010 | tcp | surf |
| 1011 | tcp | unknown |
| 1433 | tcp | ms-sql-s |
| 1556 | tcp | veritas\_pbx |
| 1801 | tcp | msmq |
| 2007 | tcp | dectalk |
| 2020 | tcp | xinupageserver |
| 2021 | tcp | servexec |
| 2103 | tcp | zephyr-clt |
| 2105 | tcp | eklogin |
| 2107 | tcp | msmq-mgmt |
| 2500 | tcp | rtsserv |
| 2525 | tcp | ms-v-worlds |
| 3011 | tcp | trusted-web |
| 3031 | tcp | eppc |
| 3211 | tcp | avsecuremgmt |
| 3268 | tcp | globalcatLDAP |
| 3269 | tcp | globalcatLDAPssl |
| 3301 | tcp | unknown |
| 3306 | tcp | mysql |
| 3389 | tcp | ms-wbt-server |
| 3800 | tcp | pwgpsi |
| 3801 | tcp | ibm-mgr |
| 3828 | tcp | neteh |
| 4000 | tcp | remoteanything |
| 4045 | tcp | lockd |
| 4848 | tcp | appserv-http |
| 5001 | tcp | commplex-link |
| 5357 | tcp | wsdapi |
| 5432 | tcp | postgresql |
| 5800 | tcp | vnc-http |
| 5900 | tcp | vnc |
| 5989 | tcp | wbem-https |
| 6000 | tcp | X11 |
| 6001 | tcp | X11:1 |
| 6101 | tcp | backupexec |
| 6646 | tcp | unknown |
| 6667 | tcp | irc |
| 6881 | tcp | bittorrent-tracker |
| 7000 | tcp | afs3-fileserver |
| 8000 | tcp | http-alt |
| 8001 | tcp | vcom-tunnel |
| 8009 | tcp | ajp13 |
| 8010 | tcp | xmpp |
| 8080 | tcp | http-proxy |
| 8081 | tcp | blackice-icecap |
| 8090 | tcp | opsmessaging |
| 8181 | tcp | intermapper |
| 8300 | tcp | tmi |
| 8443 | tcp | https-alt |
| 9000 | tcp | cslistener |
| 9010 | tcp | sdr |
| 9080 | tcp | glrpc |
| 9090 | tcp | zeus-admin |
| 9200 | tcp | wap-wsp |
| 9998 | tcp | distinct32 |
| 10001 | tcp | scp-config |
| 13782 | tcp | netbackup |
| 27000 | tcp | flexlm0 |
| 49152 | tcp | unknown |
| 49153 | tcp | unknown |
| 49154 | tcp | unknown |
| 49155 | tcp | unknown |
| 49156 | tcp | unknown |
| 49157 | tcp | unknown |
| 49159 | tcp | unknown |
| 49167 | tcp | unknown |
| 50002 | tcp | iiimsf |
| 65000 | tcp | unknown |

# Appendix

## **7.1 About Nessus**

Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Nessus is trusted by more than 30,000 organizations worldwide as one of the most widely deployed security technologies on the planet - and the gold standard for vulnerability assessment.

Reference: https://www.tenable.com/products/nessus

### **7.1.1 Nessus vulnerabilities**

As information about new vulnerabilities are discovered and released into the public domain, Tenable, Inc. research staff designs programs to enable Nessus to detect them. These programs are named plugins, and are written in the Nessus proprietary scripting language, called Nessus Attack Scripting Language (NASL). Plugins contain vulnerability information, a generic set of remediation actions, and the algorithm to test for the presence of the security issue.

Reference: https://www.tenable.com/plugins

### **7.1.2 Nessus risk score**

There are four risk levels in this document: Critical, High, Medium, and Low. There are methods for determining the risk level. Based on the Common Vulnerability Scoring System (CVSS), a standard for assessing the severity of vulnerabilities in computer systems. Regarded by the NIAC (National Infrastructure Advisory Council), expert assessments are measured in a range of 0 – 10

| **Severity** | **Description** | **Score** |
| --- | --- | --- |
| Critical | Vulnerabilities that score in the critical range usually have most of the following characteristics:   * Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices. * Exploitation is usually straightforward, in the sense that the attacker does not need any special authentication credentials or knowledge about individual victims, and does not need to persuade a target user, for example via social engineering, into performing any special functions.   For critical vulnerabilities, is advised that you patch or upgrade as soon as possible, unless you have other mitigating measures in place. For example, a mitigating factor could be if your installation is not accessible from the Internet. | 9.0 – 10.0 |
| High | Vulnerabilities that score in the high range usually have some of the following characteristics:   * The vulnerability is difficult to exploit. * Exploitation could result in elevated privileges. * Exploitation could result in a significant data loss or downtime. | 7.0 – 8.9 |
| Medium | Vulnerabilities that score in the medium range usually have some of the following characteristics:   * Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. * Denial of service vulnerabilities that are difficult to set up. * Exploits that require an attacker to reside on the same local network as the victim. * Vulnerabilities where exploitation provides only very limited access. * Vulnerabilities that require user privileges for successful exploitation. | 4.0 – 6.9 |
| Low | Vulnerabilities in the low range typically have very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local or physical system access. | 0.1 – 3.9 |

## **7.2 About Burp Suite's web vulnerability scanner**

The web vulnerability scanner behind Burp Suite's popularity has more to it than most. Burp Scanner uses PortSwigger's world-leading research to help its users find a wide range of vulnerabilities in web applications, automatically. Sitting at the core of both Burp Suite Enterprise Edition and Burp Suite Professional, Burp Scanner is the weapon of choice for over 60,000 users across more than 15,000 organizations.

Reference: https://portswigger.net/burp/vulnerability-scanner

### **7.2.1 Burp Suite's web vulnerability scanner risk score**

The level of severity for an issue that was found by a scan. The higher the severity level, the larger the impact is likely to be if an attacker is able to exploit this vulnerability. Note that the severity level is only a rough approximation based on a typical website. You should use your knowledge of the purpose and context of the associated functionality to determine how serious each issue is in your individual case.

Reference: https://portswigger.net/burp/extensibility/enterprise/graphql-api/severity.html

| **Severity** | **Description** |
| --- | --- |
| High | An attacker can **fully** compromise the confidentiality, integrity, or availability, of a target system without specialized access, user interaction or circumstances that are beyond the attacker’s control. Very likely to allow lateral movement and escalation of attack to other systems on the internal network of the vulnerable application. |
| Medium | An attacker can **partially** compromise the confidentiality, integrity, or availability, of a target system. Specialized access, user interaction, or circumstances that are beyond the attacker’s control may be required for an attack to succeed. Very likely to be used in conjunction with other vulnerabilities to escalate an attack. |
| Low | An attacker can **limitedly** compromise the confidentiality, integrity, or availability, of a target system. Specialized access, user interaction, or circumstances that are beyond the attacker’s control is required for an attack to succeed. Needs to be used in conjunction with other vulnerabilities to escalate an attack. |