**Vulnerability Assessment Report**

**For**



**SIPH phase 1 greenbone**

**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 phase 1 greenbone | | 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 | - | test | - | test |

## **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**

A picture containing text, gambling house

Description automatically generated

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 | 5 | 0 | 5 |
| 2 | - | 172.28.130.35 | 0 | 0 | 6 | 0 | 6 |
| 3 | - | 172.28.130.37 | 0 | 0 | 5 | 0 | 5 |
| 4 | - | 172.28.130.128 | 0 | 3 | 13 | 1 | 17 |
| 5 | - | 172.28.130.190 | 0 | 77 | 81 | 4 | 162 |
| 6 | - | 172.28.135.188 | 0 | 0 | 0 | 1 | 1 |
| 7 | - | 172.28.135.189 | 0 | 0 | 2 | 1 | 3 |
| 8 | - | 172.28.188.167 | 0 | 1 | 5 | 2 | 8 |
| 9 | - | 172.28.188.168 | 0 | 1 | 9 | 2 | 12 |
| 10 | - | 172.28.190.139 | 0 | 0 | 3 | 1 | 4 |
| 11 | - | 172.28.190.153 | 0 | 0 | 3 | 0 | 3 |
| **Total** | | | 0 | 82 | 132 | 12 | 226 |

## **5.3 Infrastructure Vulnerability Detail**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 1 | **Finding** | PHP 7.4.28, 8.0.x 8.0.16, 8.1.x 8.1.3 Security Update (Feb 2022) - Windows |
| **Severity** | **High** | **Port** | TCP: 2021 |
| **Target** | 172.28.130.128(2021) | | |
| **Detail** | Fix #81708: UAF due to php\_filter\_float() failing for ints. | | |
| **Solution** | Update to version 7.4.28, 8.0.16, 8.1.3 or later. | | |
| **Remark** | CVE: CVE-2021-21708 CERT: DFN-CERT-2022-0557 CERT: DFN-CERT-2022-0407 CERT: DFN-CERT-2022-0365 CERT: CB-K22/0201 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 2 | **Finding** | PHP CVE-2017-7189 Improper Input Validation Vulnerability (Windows) |
| **Severity** | **High** | **Port** | TCP: 2021 |
| **Target** | 172.28.130.128(2021) | | |
| **Detail** | main/streams/xp\_socket.c in PHP misparses fsockopen calls, such as by  interpreting fsockopen('127.0.0.1:80', 443) as if the address/port were 127.0.0.1:80:443, which is later  truncated to 127.0.0.1:80. This behavior has a security risk if the explicitly provided port number  (i.e., 443 in this example) is hardcoded into an application as a security policy, but the hostname  argument (i.e., 127.0.0.1:80 in this example) is obtained from untrusted input. | | |
| **Solution** | No solution was made available by the vendor. General solution options  are to upgrade to a newer release, disable respective features, remove the product or replace the product  by another one.   Note: PHP versions 7.0.18 and 7.1.4 introduced a fix which was reverted again in version 7.0.19 / 7.1.5 respectively  and the fix wasn't introduced again as of today (08-2020). | | |
| **Remark** | CVE: CVE-2017-7189 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 3 | **Finding** | PHP 5.3.7 - 7.3.31, 7.4.x 7.4.25, 8.0.x 8.0.12 Security Update (Oct 2021) - Windows |
| **Severity** | **High** | **Port** | TCP: 2021 |
| **Target** | 172.28.130.128(2021) | | |
| **Detail** | Fixed bug #81026 (PHP-FPM oob R/W in root process leading to  privilege escalation). | | |
| **Solution** | Update to version 7.3.32 (not released yet), 7.4.25, 8.0.12 or  later. | | |
| **Remark** | CVE: CVE-2021-21703 CERT: DFN-CERT-2022-0485 CERT: DFN-CERT-2021-2586 CERT: DFN-CERT-2021-2474 CERT: DFN-CERT-2021-2200 CERT: CB-K21/1106 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 4 | **Finding** | Apache Tomcat Privilege Escalation Vulnerability - Dec19 (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8081, 8443, 8444 |
| **Target** | 172.28.130.190(443, 8080, 8081, 8443, 8444) | | |
| **Detail** | When 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. | | |
| **Solution** | Update to version 7.0.99, 8.5.49, 9.0.29 or later. As a mitigation disable  Tomcat's JmxRemoteLifecycleListener and use the built-in remote JMX facilities provided by the JVM. | | |
| **Remark** | CVE: CVE-2019-12418 CERT: DFN-CERT-2020-1129 CERT: DFN-CERT-2020-1094 CERT: DFN-CERT-2020-0821 CERT: DFN-CERT-2020-0604 CERT: DFN-CERT-2020-0557 CERT: DFN-CERT-2020-0501 CERT: DFN-CERT-2020-0345 CERT: DFN-CERT-2020-0027 CERT: DFN-CERT-2019-2710 CERT: DFN-CERT-2019-2673 CERT: CB-K20/0309 CERT: CB-K19/1102 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 5 | **Finding** | Apache Tomcat Multiple Vulnerabilities - Feb20 (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8081, 8443, 8444 |
| **Target** | 172.28.130.190(443, 8080, 8081, 8443, 8444) | | |
| **Detail** | Apache Tomcat is prone to multiple vulnerabilities:   - HTTP request smuggling vulnerability (CVE-2020-1935)   - AJP Request Injection and potential Remote Code Execution dubbed 'Ghostcat' (CVE-2020-1938) | | |
| **Solution** | Update to version 7.0.100, 8.5.51, 9.0.31 or later. | | |
| **Remark** | CVE: CVE-2020-1935 CVE: CVE-2020-1938 CERT: DFN-CERT-2021-1736 CERT: DFN-CERT-2021-0575 CERT: DFN-CERT-2020-2482 CERT: DFN-CERT-2020-1707 CERT: DFN-CERT-2020-1706 CERT: DFN-CERT-2020-1508 CERT: DFN-CERT-2020-1413 CERT: DFN-CERT-2020-1276 CERT: DFN-CERT-2020-1134 CERT: DFN-CERT-2020-0850 CERT: DFN-CERT-2020-0835 CERT: DFN-CERT-2020-0821 CERT: DFN-CERT-2020-0569 CERT: DFN-CERT-2020-0557 CERT: DFN-CERT-2020-0501 CERT: DFN-CERT-2020-0381 CERT: CB-K20/0711 CERT: CB-K20/0705 CERT: CB-K20/0693 CERT: CB-K20/0555 CERT: CB-K20/0543 CERT: CB-K20/0165 CERT: CB-K20/0154 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 6 | **Finding** | Apache Tomcat NIO HTTP connector Information Disclosure Vulnerability (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The flaw exists due to error handling of the  send file code for the NIO HTTP connector in Apache Tomcat resulting in the  current Processor object being added to the Processor cache multiple times.  This in turn means that the same Processor could be used for concurrent requests.  Sharing a Processor can result in information leakage between requests including,  not not limited to, session ID and the response body. | | |
| **Solution** | Upgrade to Apache Tomcat version 9.0.0.M15  or 8.5.9 or 8.0.41 or 7.0.75 or 6.0.50 or later. | | |
| **Remark** | CVE: CVE-2016-8745 CERT: DFN-CERT-2018-0729 CERT: DFN-CERT-2017-1822 CERT: DFN-CERT-2017-1095 CERT: DFN-CERT-2017-1068 CERT: DFN-CERT-2017-0828 CERT: DFN-CERT-2017-0456 CERT: DFN-CERT-2017-0404 CERT: DFN-CERT-2017-0308 CERT: DFN-CERT-2017-0137 CERT: DFN-CERT-2017-0095 CERT: DFN-CERT-2016-2037 CERT: CB-K18/0605 CERT: CB-K17/1746 CERT: CB-K17/1060 CERT: CB-K17/1033 CERT: CB-K17/0801 CERT: CB-K17/0444 CERT: CB-K17/0397 CERT: CB-K17/0303 CERT: CB-K17/0133 CERT: CB-K17/0090 CERT: CB-K16/1929 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 7 | **Finding** | Apache Tomcat Denial Of Service Vulnerability - Jun15 (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The flaw is due to improper handling of  cases where an HTTP response occurs before finishing the reading of an  entire request body. | | |
| **Solution** | Upgrade to version 6.0.44 or 7.0.55 or  8.0.9 or later. | | |
| **Remark** | CVE: CVE-2014-0230 CERT: DFN-CERT-2016-0556 CERT: DFN-CERT-2016-0537 CERT: DFN-CERT-2016-0518 CERT: DFN-CERT-2016-0042 CERT: DFN-CERT-2015-1965 CERT: DFN-CERT-2015-1950 CERT: DFN-CERT-2015-1632 CERT: DFN-CERT-2015-1251 CERT: DFN-CERT-2015-1070 CERT: DFN-CERT-2015-0928 CERT: DFN-CERT-2015-0655 CERT: CB-K16/0513 CERT: CB-K16/0496 CERT: CB-K16/0476 CERT: CB-K16/0034 CERT: CB-K15/1860 CERT: CB-K15/1841 CERT: CB-K15/1550 CERT: CB-K15/1182 CERT: CB-K15/1016 CERT: CB-K15/0874 CERT: CB-K15/0628 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 8 | **Finding** | Apache Tomcat Session Fixation Vulnerability - Dec19 (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8081, 8443, 8444 |
| **Target** | 172.28.130.190(443, 8080, 8081, 8443, 8444) | | |
| **Detail** | 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. | | |
| **Solution** | Update to version 7.0.99, 8.5.50, 9.0.30 or later. | | |
| **Remark** | CVE: CVE-2019-17563 CERT: DFN-CERT-2021-0575 CERT: DFN-CERT-2020-2132 CERT: DFN-CERT-2020-1134 CERT: DFN-CERT-2020-1129 CERT: DFN-CERT-2020-0821 CERT: DFN-CERT-2020-0780 CERT: DFN-CERT-2020-0775 CERT: DFN-CERT-2020-0557 CERT: DFN-CERT-2020-0501 CERT: DFN-CERT-2020-0345 CERT: DFN-CERT-2020-0027 CERT: DFN-CERT-2019-2710 CERT: DFN-CERT-2019-2673 CERT: CB-K21/0071 CERT: CB-K20/1030 CERT: CB-K20/0318 CERT: CB-K20/0309 CERT: CB-K19/1102 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 9 | **Finding** | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS |
| **Severity** | **High** | **Port** | TCP: 443, 8443 |
| **Target** | 172.28.130.190(8443), 172.28.188.167(443), 172.28.188.168(443) | | |
| **Detail** | These rules are applied for the evaluation of the vulnerable cipher suites:   - 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183). | | |
| **Solution** | The configuration of this services should be changed so  that it does not accept the listed cipher suites anymore.   Please see the references for more resources supporting you with this task. | | |
| **Remark** | CVE: CVE-2016-2183 CVE: CVE-2016-6329 CVE: CVE-2020-12872 CERT: DFN-CERT-2021-1618 CERT: DFN-CERT-2021-0775 CERT: DFN-CERT-2021-0770 CERT: DFN-CERT-2021-0274 CERT: DFN-CERT-2020-2141 CERT: DFN-CERT-2020-0368 CERT: DFN-CERT-2019-1455 CERT: DFN-CERT-2019-0068 CERT: DFN-CERT-2018-1296 CERT: DFN-CERT-2018-0323 CERT: DFN-CERT-2017-2070 CERT: DFN-CERT-2017-1954 CERT: DFN-CERT-2017-1885 CERT: DFN-CERT-2017-1831 CERT: DFN-CERT-2017-1821 CERT: DFN-CERT-2017-1785 CERT: DFN-CERT-2017-1626 CERT: DFN-CERT-2017-1326 CERT: DFN-CERT-2017-1239 CERT: DFN-CERT-2017-1238 CERT: DFN-CERT-2017-1090 CERT: DFN-CERT-2017-1060 CERT: DFN-CERT-2017-0968 CERT: DFN-CERT-2017-0947 CERT: DFN-CERT-2017-0946 CERT: DFN-CERT-2017-0904 CERT: DFN-CERT-2017-0816 CERT: DFN-CERT-2017-0746 CERT: DFN-CERT-2017-0677 CERT: DFN-CERT-2017-0675 CERT: DFN-CERT-2017-0611 CERT: DFN-CERT-2017-0609 CERT: DFN-CERT-2017-0522 CERT: DFN-CERT-2017-0519 CERT: DFN-CERT-2017-0482 CERT: DFN-CERT-2017-0351 CERT: DFN-CERT-2017-0090 CERT: DFN-CERT-2017-0089 CERT: DFN-CERT-2017-0088 CERT: DFN-CERT-2017-0086 CERT: DFN-CERT-2016-1943 CERT: DFN-CERT-2016-1937 CERT: DFN-CERT-2016-1732 CERT: DFN-CERT-2016-1726 CERT: DFN-CERT-2016-1715 CERT: DFN-CERT-2016-1714 CERT: DFN-CERT-2016-1588 CERT: DFN-CERT-2016-1555 CERT: DFN-CERT-2016-1391 CERT: DFN-CERT-2016-1378 CERT: CB-K21/1094 CERT: CB-K20/1023 CERT: CB-K20/0321 CERT: CB-K20/0314 CERT: CB-K20/0157 CERT: CB-K19/0618 CERT: CB-K19/0615 CERT: CB-K18/0296 CERT: CB-K17/1980 CERT: CB-K17/1871 CERT: CB-K17/1803 CERT: CB-K17/1753 CERT: CB-K17/1750 CERT: CB-K17/1709 CERT: CB-K17/1558 CERT: CB-K17/1273 CERT: CB-K17/1202 CERT: CB-K17/1196 CERT: CB-K17/1055 CERT: CB-K17/1026 CERT: CB-K17/0939 CERT: CB-K17/0917 CERT: CB-K17/0915 CERT: CB-K17/0877 CERT: CB-K17/0796 CERT: CB-K17/0724 CERT: CB-K17/0661 CERT: CB-K17/0657 CERT: CB-K17/0582 CERT: CB-K17/0581 CERT: CB-K17/0506 CERT: CB-K17/0504 CERT: CB-K17/0467 CERT: CB-K17/0345 CERT: CB-K17/0098 CERT: CB-K17/0089 CERT: CB-K17/0086 CERT: CB-K17/0082 CERT: CB-K16/1837 CERT: CB-K16/1830 CERT: CB-K16/1635 CERT: CB-K16/1630 CERT: CB-K16/1624 CERT: CB-K16/1622 CERT: CB-K16/1500 CERT: CB-K16/1465 CERT: CB-K16/1307 CERT: CB-K16/1296 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 10 | **Finding** | Apache Tomcat Security Bypass Vulnerability (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The error page mechanism of the Java Servlet  Specification requires that, when an error occurs and an error page is  configured for the error that occurred, the original request and response are  forwarded to the error page. This means that the request is presented to the  error page with the original HTTP method. If the error page is a static file,  expected behaviour is to serve content of the file as if processing a GET request,  regardless of the actual HTTP method. Tomcat's Default Servlet did not do this.  Depending on the original request this could lead to unexpected and undesirable  results for static error pages including, if the DefaultServlet is configured to  permit writes, the replacement or removal of the custom error page | | |
| **Solution** | Upgrade to version 9.0.0.M21, or 8.5.15,  or 8.0.44, or 7.0.78 or later. | | |
| **Remark** | CVE: CVE-2017-5664 CERT: DFN-CERT-2018-1274 CERT: DFN-CERT-2018-0729 CERT: DFN-CERT-2018-0513 CERT: DFN-CERT-2018-0077 CERT: DFN-CERT-2018-0051 CERT: DFN-CERT-2017-2116 CERT: DFN-CERT-2017-2106 CERT: DFN-CERT-2017-1914 CERT: DFN-CERT-2017-1827 CERT: DFN-CERT-2017-1558 CERT: DFN-CERT-2017-1485 CERT: DFN-CERT-2017-1300 CERT: DFN-CERT-2017-1288 CERT: DFN-CERT-2017-1011 CERT: CB-K18/0605 CERT: CB-K18/0603 CERT: CB-K18/0478 CERT: CB-K18/0066 CERT: CB-K18/0047 CERT: CB-K17/2024 CERT: CB-K17/2017 CERT: CB-K17/1831 CERT: CB-K17/1748 CERT: CB-K17/1492 CERT: CB-K17/1423 CERT: CB-K17/1257 CERT: CB-K17/1246 CERT: CB-K17/0977 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 11 | **Finding** | Apache Tomcat Security Manager Bypass Vulnerability - 01 - Feb16 (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The flaw exists due to an improper validation  of several session persistence mechanisms and the StatusManagerServlet loaded  by a web application when a security manager was configured. | | |
| **Solution** | Upgrade to version 6.0.45 or 7.0.68 or  8.0.32 or 9.0.0.M3 or later. | | |
| **Remark** | CVE: CVE-2016-0714 CVE: CVE-2016-0706 CERT: DFN-CERT-2017-1821 CERT: DFN-CERT-2017-0677 CERT: DFN-CERT-2017-0090 CERT: DFN-CERT-2016-1905 CERT: DFN-CERT-2016-1823 CERT: DFN-CERT-2016-1726 CERT: DFN-CERT-2016-1715 CERT: DFN-CERT-2016-1661 CERT: DFN-CERT-2016-1059 CERT: DFN-CERT-2016-0842 CERT: DFN-CERT-2016-0807 CERT: DFN-CERT-2016-0537 CERT: DFN-CERT-2016-0518 CERT: DFN-CERT-2016-0314 CERT: CB-K17/1750 CERT: CB-K17/0661 CERT: CB-K17/0098 CERT: CB-K16/1799 CERT: CB-K16/1758 CERT: CB-K16/1630 CERT: CB-K16/1622 CERT: CB-K16/1568 CERT: CB-K16/0993 CERT: CB-K16/0789 CERT: CB-K16/0758 CERT: CB-K16/0496 CERT: CB-K16/0476 CERT: CB-K16/0292 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 12 | **Finding** | Apache Tomcat SecurityManager Information Disclosure Vulnerability (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | A some calls to application listeners  did not use the appropriate facade object. When running an untrusted  application under a SecurityManager, it was therefore possible for  that untrusted application to retain a reference to the request or  response object and thereby access and/or modify information associated  with another web application. | | |
| **Solution** | Upgrade to version 9.0.0.M18,  8.5.12, 8.0.42, 7.0.76 or later. | | |
| **Remark** | CVE: CVE-2017-5648 CERT: DFN-CERT-2018-0051 CERT: DFN-CERT-2017-1300 CERT: DFN-CERT-2017-1288 CERT: DFN-CERT-2017-1095 CERT: DFN-CERT-2017-0828 CERT: DFN-CERT-2017-0624 CERT: CB-K18/0047 CERT: CB-K17/1257 CERT: CB-K17/1246 CERT: CB-K17/1060 CERT: CB-K17/0801 CERT: CB-K17/0604 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 13 | **Finding** | Apache Tomcat HTTP/2 Vulnerability - Dec20 (Windows) |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | It was discovered that Apache Tomcat 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. | | |
| **Solution** | Update to version 8.5.60, 9.0.40, 10.0.0-M10 or later. | | |
| **Remark** | CVE: CVE-2020-17527 CERT: DFN-CERT-2021-2620 CERT: DFN-CERT-2021-0821 CERT: DFN-CERT-2021-0820 CERT: DFN-CERT-2021-0338 CERT: DFN-CERT-2021-0134 CERT: DFN-CERT-2021-0034 CERT: DFN-CERT-2020-2646 CERT: CB-K21/0421 CERT: CB-K21/0418 CERT: CB-K20/1195 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 14 | **Finding** | Apache Tomcat RCE Vulnerability (Mar21) - Windows |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8081, 8443, 8444 |
| **Target** | 172.28.130.190(443, 8080, 8081, 8443, 8444) | | |
| **Detail** | The fix for CVE-2020-9484 was incomplete. When using a highly unlikely  configuration edge case, the Tomcat instance is still vulnerable to CVE-2020-9484. Note that both the  previously published prerequisites for CVE-2020-9484 also apply to this issue. | | |
| **Solution** | Update to version 7.0.108, 8.5.63, 9.0.43, 10.0.2 or later. | | |
| **Remark** | CVE: CVE-2021-25329 CERT: DFN-CERT-2021-1904 CERT: DFN-CERT-2021-1403 CERT: DFN-CERT-2021-0903 CERT: DFN-CERT-2021-0835 CERT: DFN-CERT-2021-0807 CERT: DFN-CERT-2021-0714 CERT: DFN-CERT-2021-0544 CERT: DFN-CERT-2021-0445 CERT: CB-K21/0222 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 15 | **Finding** | Apache Tomcat DoS Vulnerability - June19 (Windows) |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | 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  are able to cause server-side threads to block eventually leading to thread exhaustion and a DoS. | | |
| **Solution** | Update to version 8.5.41, 9.0.20 or later. | | |
| **Remark** | CVE: CVE-2019-10072 CERT: DFN-CERT-2020-0501 CERT: DFN-CERT-2020-0088 CERT: DFN-CERT-2020-0027 CERT: DFN-CERT-2019-2457 CERT: DFN-CERT-2019-2149 CERT: DFN-CERT-2019-1895 CERT: DFN-CERT-2019-1472 CERT: DFN-CERT-2019-1268 CERT: CB-K20/1008 CERT: CB-K20/0029 CERT: CB-K19/0915 CERT: CB-K19/0523 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 16 | **Finding** | Apache Tomcat DoS Vulnerability - June20 (Windows) |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | A specially crafted sequence of HTTP/2 requests sent to Apache Tomcat could  trigger high CPU usage for several seconds. If a sufficient number of such requests were made on concurrent  HTTP/2 connections, the server could become unresponsive. | | |
| **Solution** | Update to version 8.5.56, 9.0.36, 10.0.0-M6 or later. | | |
| **Remark** | CVE: CVE-2020-11996 CERT: DFN-CERT-2021-1736 CERT: DFN-CERT-2021-0043 CERT: DFN-CERT-2020-2006 CERT: DFN-CERT-2020-1575 CERT: DFN-CERT-2020-1490 CERT: DFN-CERT-2020-1358 CERT: CB-K20/1017 CERT: CB-K20/0637 CERT: CB-K20/0636 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 17 | **Finding** | Apache Tomcat RCE Vulnerability - May20 (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8081, 8443, 8444 |
| **Target** | 172.28.130.190(443, 8080, 8081, 8443, 8444) | | |
| **Detail** | If:   - an attacker is able to control the contents and name of a file on the server and   - the server is configured to use the PersistenceManager with a FileStore and   - 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   - 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 all of conditions must be true for the attack to  succeed. | | |
| **Solution** | Update to version 7.0.104, 8.5.55, 9.0.35, 10.0.0-M5 or later. | | |
| **Remark** | CVE: CVE-2020-9484 CERT: DFN-CERT-2021-1736 CERT: DFN-CERT-2020-2286 CERT: DFN-CERT-2020-1706 CERT: DFN-CERT-2020-1635 CERT: DFN-CERT-2020-1575 CERT: DFN-CERT-2020-1490 CERT: DFN-CERT-2020-1289 CERT: DFN-CERT-2020-1134 CERT: DFN-CERT-2020-1129 CERT: DFN-CERT-2020-1094 CERT: DFN-CERT-2020-1086 CERT: CB-K21/1094 CERT: CB-K21/0069 CERT: CB-K20/1017 CERT: CB-K20/0494 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 18 | **Finding** | Apache Tomcat DoS Vulnerability - March19 (Windows) |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | The HTTP/2 implementation accepts streams with excessive numbers of SETTINGS  frames and also permitts clients to keep streams open without reading/writing request/response data. By keeping  streams open for requests that utilises the Servlet API's blocking I/O, clients are able to cause server-side  threads to block eventually leading to thread exhaustion and a DoS. | | |
| **Solution** | Update to version 8.5.38, 9.0.16 or later. | | |
| **Remark** | CVE: CVE-2019-0199 CERT: DFN-CERT-2019-2710 CERT: DFN-CERT-2019-1895 CERT: DFN-CERT-2019-1755 CERT: DFN-CERT-2019-1472 CERT: DFN-CERT-2019-1231 CERT: DFN-CERT-2019-1095 CERT: DFN-CERT-2019-0594 CERT: CB-K20/0543 CERT: CB-K20/0029 CERT: CB-K19/0235 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 19 | **Finding** | Apache Tomcat Hostname Verification Security Bypass Vulnerability (Windows) |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | The flaw exists due to a missing host name  verification when using TLS with the WebSocket client. | | |
| **Solution** | Upgrade to Apache Tomcat version 9.0.10 or  8.5.32 or 8.0.53 or 7.0.90 or later. Please see the references for more information. | | |
| **Remark** | CVE: CVE-2018-8034 CERT: DFN-CERT-2019-2418 CERT: DFN-CERT-2019-1627 CERT: DFN-CERT-2019-1237 CERT: DFN-CERT-2019-0951 CERT: DFN-CERT-2019-0451 CERT: DFN-CERT-2019-0147 CERT: DFN-CERT-2018-2165 CERT: DFN-CERT-2018-2142 CERT: DFN-CERT-2018-1753 CERT: DFN-CERT-2018-1471 CERT: DFN-CERT-2018-1443 CERT: DFN-CERT-2018-1262 CERT: CB-K19/0907 CERT: CB-K19/0616 CERT: CB-K19/0320 CERT: CB-K18/1005 CERT: CB-K18/0809 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 20 | **Finding** | Apache Tomcat VirtualDirContext Information Disclosure Vulnerability (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The flaw is due to an improper serving of  files via 'VirtualDirContext'. | | |
| **Solution** | Upgrade to Tomcat version 7.0.81 or later. | | |
| **Remark** | CVE: CVE-2017-12616 CERT: DFN-CERT-2018-1253 CERT: DFN-CERT-2018-1038 CERT: DFN-CERT-2018-0455 CERT: DFN-CERT-2017-2116 CERT: DFN-CERT-2017-1665 CERT: CB-K18/0420 CERT: CB-K17/2024 CERT: CB-K17/1593 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 21 | **Finding** | Apache Tomcat RCE Vulnerability - April19 (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8081, 8443, 8444 |
| **Target** | 172.28.130.190(443, 8080, 8081, 8443, 8444) | | |
| **Detail** | When running on Windows with enableCmdLineArguments enabled, the CGI Servlet  is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows.  The CGI Servlet is disabled by default. The CGI option enableCmdLineArguments is disabled by default in Tomcat. | | |
| **Solution** | Update to version 7.0.94, 8.5.40, 9.0.19 or later. | | |
| **Remark** | CVE: CVE-2019-0232 CERT: DFN-CERT-2019-1398 CERT: DFN-CERT-2019-0732 CERT: CB-K20/0029 CERT: CB-K19/0920 CERT: CB-K19/0616 CERT: CB-K19/0306 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 22 | **Finding** | Apache Tomcat Information Disclosure Vulnerability (Mar21) - Windows |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | When responding to new h2c connection requests, Apache Tomcat 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. | | |
| **Solution** | Update to version 8.5.63, 9.0.43, 10.0.2 or later. | | |
| **Remark** | CVE: CVE-2021-25122 CERT: DFN-CERT-2021-2191 CERT: DFN-CERT-2021-1904 CERT: DFN-CERT-2021-1537 CERT: DFN-CERT-2021-1536 CERT: DFN-CERT-2021-1403 CERT: DFN-CERT-2021-0810 CERT: DFN-CERT-2021-0807 CERT: DFN-CERT-2021-0544 CERT: DFN-CERT-2021-0445 CERT: CB-K21/1094 CERT: CB-K21/1081 CERT: CB-K21/0770 CERT: CB-K21/0222 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 23 | **Finding** | Apache Tomcat DoS Vulnerability (Sep 2021) - Windows |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL  for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a  denial of service. | | |
| **Solution** | Update to version 8.5.64, 9.0.44, 10.0.4 or later. | | |
| **Remark** | CVE: CVE-2021-41079 CERT: DFN-CERT-2021-2297 CERT: DFN-CERT-2021-2169 CERT: DFN-CERT-2021-1990 CERT: CB-K21/0983 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 24 | **Finding** | Apache Tomcat pipelined Requests Information Disclosure Vulnerability (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | A bug in the handling of the pipelined  requests when send file was used resulted in the pipelined request being  lost when send file processing of the previous request completed. | | |
| **Solution** | Upgrade to version 9.0.0.M19,  8.5.13, 8.0.43, 7.0.77, 6.0.53 or later. | | |
| **Remark** | CVE: CVE-2017-5647 CERT: DFN-CERT-2018-0051 CERT: DFN-CERT-2017-1914 CERT: DFN-CERT-2017-1485 CERT: DFN-CERT-2017-1288 CERT: DFN-CERT-2017-1243 CERT: DFN-CERT-2017-1095 CERT: DFN-CERT-2017-1068 CERT: DFN-CERT-2017-0828 CERT: DFN-CERT-2017-0624 CERT: CB-K18/0047 CERT: CB-K17/1831 CERT: CB-K17/1423 CERT: CB-K17/1246 CERT: CB-K17/1205 CERT: CB-K17/1060 CERT: CB-K17/1033 CERT: CB-K17/0801 CERT: CB-K17/0604 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 25 | **Finding** | Apache Tomcat Multiple DoS Vulnerabilities - July20 (Windows) |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | The following vulnerabilitities exist:   - HTTP/2 Denial of Service (CVE-2020-13934)   - WebSocket Denial of Service (CVE-2020-13935) | | |
| **Solution** | Update to version 8.5.57, 9.0.37, 10.0.0-M7 or later. | | |
| **Remark** | CVE: CVE-2020-13934 CVE: CVE-2020-13935 CERT: DFN-CERT-2021-1736 CERT: DFN-CERT-2021-0714 CERT: DFN-CERT-2021-0132 CERT: DFN-CERT-2020-2295 CERT: DFN-CERT-2020-2287 CERT: DFN-CERT-2020-2132 CERT: DFN-CERT-2020-2006 CERT: DFN-CERT-2020-1761 CERT: DFN-CERT-2020-1707 CERT: DFN-CERT-2020-1706 CERT: DFN-CERT-2020-1575 CERT: DFN-CERT-2020-1511 CERT: CB-K20/1030 CERT: CB-K20/1021 CERT: CB-K20/1017 CERT: CB-K20/0717 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 26 | **Finding** | Apache Tomcat DoS Vulnerability (Apr 2014) - Windows |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | MultipartStream.java in Apache Commons FileUpload before 1.3.1,  as used in Apache Tomcat, allows remote attackers to cause a denial of service (infinite loop and  CPU consumption) via a crafted Content-Type header that bypasses a loop's intended exit conditions. | | |
| **Solution** | Update to version 7.0.52, 8.0.3 or later. | | |
| **Remark** | CVE: CVE-2014-0050 CERT: DFN-CERT-2015-0712 CERT: DFN-CERT-2015-0556 CERT: DFN-CERT-2014-1364 CERT: DFN-CERT-2014-1359 CERT: DFN-CERT-2014-1238 CERT: DFN-CERT-2014-1184 CERT: DFN-CERT-2014-0560 CERT: DFN-CERT-2014-0536 CERT: DFN-CERT-2014-0534 CERT: DFN-CERT-2014-0452 CERT: DFN-CERT-2014-0433 CERT: DFN-CERT-2014-0280 CERT: DFN-CERT-2014-0156 CERT: CB-K15/0678 CERT: CB-K15/0544 CERT: CB-K14/1298 CERT: CB-K14/1297 CERT: CB-K14/1178 CERT: CB-K14/1126 CERT: CB-K14/0538 CERT: CB-K14/0514 CERT: CB-K14/0513 CERT: CB-K14/0437 CERT: CB-K14/0417 CERT: CB-K14/0272 CERT: CB-K14/0153 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 27 | **Finding** | Apache Tomcat HTTP Request Line Information Disclosure Vulnerability (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The code that parsed the HTTP request line  permitted invalid characters. This could be exploited, in conjunction with a  proxy that also permitted the invalid characters but with a different  interpretation, to inject data into the HTTP response. | | |
| **Solution** | Upgrade to version 9.0.0.M13,  8.5.8, 8.0.39, 7.0.73, 6.0.48 or later. | | |
| **Remark** | CVE: CVE-2016-6816 CERT: DFN-CERT-2017-1822 CERT: DFN-CERT-2017-1095 CERT: DFN-CERT-2017-1068 CERT: DFN-CERT-2017-0456 CERT: DFN-CERT-2017-0404 CERT: DFN-CERT-2017-0203 CERT: DFN-CERT-2017-0137 CERT: DFN-CERT-2017-0095 CERT: DFN-CERT-2016-2090 CERT: DFN-CERT-2016-2035 CERT: DFN-CERT-2016-1922 CERT: CB-K17/1746 CERT: CB-K17/1060 CERT: CB-K17/1033 CERT: CB-K17/0444 CERT: CB-K17/0397 CERT: CB-K17/0198 CERT: CB-K17/0133 CERT: CB-K17/0090 CERT: CB-K16/1976 CERT: CB-K16/1927 CERT: CB-K16/1815 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 28 | **Finding** | Apache Tomcat AJP RCE Vulnerability (Ghostcat) |
| **Severity** | **High** | **Port** | TCP: 8009 |
| **Target** | 172.28.130.190(8009) | | |
| **Detail** | Apache Tomcat server has a file containing vulnerability, which can be used by  an attacker to read or include any files in all webapp directories on Tomcat, such as webapp configuration files  or source code. | | |
| **Solution** | Update Apache Tomcat to version 7.0.100, 8.5.51, 9.0.31 or later. For other products  using Tomcat please contact the vendor for more information on fixed versions. | | |
| **Remark** | CVE: CVE-2020-1938 CERT: DFN-CERT-2021-1736 CERT: DFN-CERT-2020-1508 CERT: DFN-CERT-2020-1413 CERT: DFN-CERT-2020-1276 CERT: DFN-CERT-2020-1134 CERT: DFN-CERT-2020-0850 CERT: DFN-CERT-2020-0835 CERT: DFN-CERT-2020-0821 CERT: DFN-CERT-2020-0569 CERT: DFN-CERT-2020-0557 CERT: DFN-CERT-2020-0501 CERT: DFN-CERT-2020-0381 CERT: CB-K20/0711 CERT: CB-K20/0705 CERT: CB-K20/0693 CERT: CB-K20/0555 CERT: CB-K20/0543 CERT: CB-K20/0154 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 29 | **Finding** | DCE/RPC and MSRPC Services Enumeration Reporting |
| **Severity** | **Medium** | **Port** | TCP: 135 |
| **Target** | 172.28.130.33(135), 172.28.130.35(135), 172.28.130.37(135), 172.28.130.128(135), 172.28.130.190(135), 172.28.135.189(135), 172.28.190.153(135) | | |
| **Detail** |  | | |
| **Solution** | Filter incoming traffic to this ports. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 30 | **Finding** | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection |
| **Severity** | **Medium** | **Port** | TCP: 443, 636, 3269, 3389, 3978, 8443, 8444 |
| **Target** | 172.28.130.33(636, 3269, 3389), 172.28.130.128(3389), 172.28.130.190(3389, 8443, 8444), 172.28.135.189(3389), 172.28.188.167(443), 172.28.188.168(443, 3978), 172.28.190.139(3389), 172.28.190.153(443, 3389) | | |
| **Detail** | The TLSv1.0 and TLSv1.1 protocols contain known cryptographic  flaws like:   - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)   - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy  Encryption (FREAK) | | |
| **Solution** | It is recommended to disable the deprecated TLSv1.0 and/or  TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more  information. | | |
| **Remark** | CVE: CVE-2011-3389 CVE: CVE-2015-0204 CERT: DFN-CERT-2020-0177 CERT: DFN-CERT-2020-0111 CERT: DFN-CERT-2019-0068 CERT: DFN-CERT-2018-1441 CERT: DFN-CERT-2018-1408 CERT: DFN-CERT-2016-1372 CERT: DFN-CERT-2016-1164 CERT: DFN-CERT-2016-0388 CERT: DFN-CERT-2015-1853 CERT: DFN-CERT-2015-1332 CERT: DFN-CERT-2015-0884 CERT: DFN-CERT-2015-0800 CERT: DFN-CERT-2015-0758 CERT: DFN-CERT-2015-0567 CERT: DFN-CERT-2015-0544 CERT: DFN-CERT-2015-0530 CERT: DFN-CERT-2015-0396 CERT: DFN-CERT-2015-0375 CERT: DFN-CERT-2015-0374 CERT: DFN-CERT-2015-0305 CERT: DFN-CERT-2015-0199 CERT: DFN-CERT-2015-0079 CERT: DFN-CERT-2015-0021 CERT: DFN-CERT-2014-1414 CERT: DFN-CERT-2013-1847 CERT: DFN-CERT-2013-1792 CERT: DFN-CERT-2012-1979 CERT: DFN-CERT-2012-1829 CERT: DFN-CERT-2012-1530 CERT: DFN-CERT-2012-1380 CERT: DFN-CERT-2012-1377 CERT: DFN-CERT-2012-1292 CERT: DFN-CERT-2012-1214 CERT: DFN-CERT-2012-1213 CERT: DFN-CERT-2012-1180 CERT: DFN-CERT-2012-1156 CERT: DFN-CERT-2012-1155 CERT: DFN-CERT-2012-1039 CERT: DFN-CERT-2012-0956 CERT: DFN-CERT-2012-0908 CERT: DFN-CERT-2012-0868 CERT: DFN-CERT-2012-0867 CERT: DFN-CERT-2012-0848 CERT: DFN-CERT-2012-0838 CERT: DFN-CERT-2012-0776 CERT: DFN-CERT-2012-0722 CERT: DFN-CERT-2012-0638 CERT: DFN-CERT-2012-0627 CERT: DFN-CERT-2012-0451 CERT: DFN-CERT-2012-0418 CERT: DFN-CERT-2012-0354 CERT: DFN-CERT-2012-0234 CERT: DFN-CERT-2012-0221 CERT: DFN-CERT-2012-0177 CERT: DFN-CERT-2012-0170 CERT: DFN-CERT-2012-0146 CERT: DFN-CERT-2012-0142 CERT: DFN-CERT-2012-0126 CERT: DFN-CERT-2012-0123 CERT: DFN-CERT-2012-0095 CERT: DFN-CERT-2012-0051 CERT: DFN-CERT-2012-0047 CERT: DFN-CERT-2012-0021 CERT: DFN-CERT-2011-1953 CERT: DFN-CERT-2011-1946 CERT: DFN-CERT-2011-1844 CERT: DFN-CERT-2011-1826 CERT: DFN-CERT-2011-1774 CERT: DFN-CERT-2011-1743 CERT: DFN-CERT-2011-1738 CERT: DFN-CERT-2011-1706 CERT: DFN-CERT-2011-1628 CERT: DFN-CERT-2011-1627 CERT: DFN-CERT-2011-1619 CERT: DFN-CERT-2011-1482 CERT: CB-K18/0799 CERT: CB-K16/1289 CERT: CB-K16/1096 CERT: CB-K15/1751 CERT: CB-K15/1266 CERT: CB-K15/0850 CERT: CB-K15/0764 CERT: CB-K15/0720 CERT: CB-K15/0548 CERT: CB-K15/0526 CERT: CB-K15/0509 CERT: CB-K15/0493 CERT: CB-K15/0384 CERT: CB-K15/0365 CERT: CB-K15/0364 CERT: CB-K15/0302 CERT: CB-K15/0192 CERT: CB-K15/0079 CERT: CB-K15/0016 CERT: CB-K14/1342 CERT: CB-K14/0231 CERT: CB-K13/0845 CERT: CB-K13/0796 CERT: CB-K13/0790 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 31 | **Finding** | Cleartext Transmission of Sensitive Information via HTTP |
| **Severity** | **Medium** | **Port** | TCP: 80, 2021, 6161, 8080 |
| **Target** | 172.28.130.33(6161), 172.28.130.35(80), 172.28.130.128(2021), 172.28.130.190(8080) | | |
| **Detail** |  | | |
| **Solution** | Enforce the transmission of sensitive data via an encrypted SSL/TLS connection.  Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before  allowing to input sensitive data into the mentioned functions. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 32 | **Finding** | SMTP Server on non standard port |
| **Severity** | **Medium** | **Port** | TCP: 475, 476, 477, 2525 |
| **Target** | 172.28.130.35(475, 476, 477, 2525), 172.28.130.37(475, 476, 477, 2525) | | |
| **Detail** |  | | |
| **Solution** | Check and clean your configuration. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 33 | **Finding** | FTP Unencrypted Cleartext Login |
| **Severity** | **Medium** | **Port** | TCP: 21 |
| **Target** | 172.28.130.128(21) | | |
| **Detail** |  | | |
| **Solution** | Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see  the manual of the FTP service for more information. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 34 | **Finding** | QuickPHP index.php Remote Source Code Disclosure Vulnerability |
| **Severity** | **Medium** | **Port** | TCP: 2020 |
| **Target** | 172.28.130.128(2020) | | |
| **Detail** |  | | |
| **Solution** | No known solution was made available for at least one year since the  disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to  upgrade to a newer release, disable respective features, remove the product or replace the product by  another one. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 35 | **Finding** | PHP 7.3.28, 7.4.x 7.4.18 IMAP Header Injection Vulnerability (Apr 2021) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 2021 |
| **Target** | 172.28.130.128(2021) | | |
| **Detail** |  | | |
| **Solution** | Update to version 7.3.28, 7.4.18 or later. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 36 | **Finding** | PHP 7.3.30, 7.4.x 7.4.23, 8.0.x 8.0.10 Security Update (Aug 2021) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 2021 |
| **Target** | 172.28.130.128(2021) | | |
| **Detail** |  | | |
| **Solution** | Update to version 7.3.30, 7.4.23, 8.0.10 or later. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 37 | **Finding** | PHP 7.3.33, 7.4.x 7.4.26, 8.0.x 8.0.13 Security Update (Nov 2021) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 2021 |
| **Target** | 172.28.130.128(2021) | | |
| **Detail** | Fixed bug #79971 (special character is breaking the path in xml  function). | | |
| **Solution** | Update to version 7.3.33, 7.4.26, 8.0.13 or later. | | |
| **Remark** | CVE: CVE-2021-21707 CERT: DFN-CERT-2022-0557 CERT: DFN-CERT-2022-0485 CERT: DFN-CERT-2022-0455 CERT: DFN-CERT-2022-0431 CERT: DFN-CERT-2022-0407 CERT: DFN-CERT-2022-0110 CERT: DFN-CERT-2021-2474 CERT: DFN-CERT-2021-2436 CERT: CB-K21/1213 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 38 | **Finding** | Sensitive File Disclosure (HTTP) |
| **Severity** | **Medium** | **Port** | TCP: 2020 |
| **Target** | 172.28.130.128(2020) | | |
| **Detail** |  | | |
| **Solution** | The sensitive files shouldn't be accessible via a web server.  Restrict access to it or remove it completely. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 39 | **Finding** | SSL/TLS: Report Weak Cipher Suites |
| **Severity** | **Medium** | **Port** | TCP: 443, 3389 |
| **Target** | 172.28.130.128(3389), 172.28.188.167(443), 172.28.188.168(443), 172.28.190.139(3389) | | |
| **Detail** | These rules are applied for the evaluation of the cryptographic  strength:   - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)   - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods  and therefore considered as weak (CVE-2015-4000)   - 1024 bit RSA authentication is considered to be insecure and therefore as weak   - Any cipher considered to be secure for only the next 10 years is considered as medium   - Any other cipher is considered as strong | | |
| **Solution** | The configuration of this services should be changed so  that it does not accept the listed weak cipher suites anymore.   Please see the references for more resources supporting you with this task. | | |
| **Remark** | CVE: CVE-2013-2566 CVE: CVE-2015-2808 CVE: CVE-2015-4000 CERT: DFN-CERT-2021-0775 CERT: DFN-CERT-2020-1561 CERT: DFN-CERT-2020-1276 CERT: DFN-CERT-2017-1821 CERT: DFN-CERT-2016-1692 CERT: DFN-CERT-2016-1648 CERT: DFN-CERT-2016-1168 CERT: DFN-CERT-2016-0665 CERT: DFN-CERT-2016-0642 CERT: DFN-CERT-2016-0184 CERT: DFN-CERT-2016-0135 CERT: DFN-CERT-2016-0101 CERT: DFN-CERT-2016-0035 CERT: DFN-CERT-2015-1853 CERT: DFN-CERT-2015-1679 CERT: DFN-CERT-2015-1632 CERT: DFN-CERT-2015-1608 CERT: DFN-CERT-2015-1542 CERT: DFN-CERT-2015-1518 CERT: DFN-CERT-2015-1406 CERT: DFN-CERT-2015-1341 CERT: DFN-CERT-2015-1194 CERT: DFN-CERT-2015-1144 CERT: DFN-CERT-2015-1113 CERT: DFN-CERT-2015-1078 CERT: DFN-CERT-2015-1067 CERT: DFN-CERT-2015-1038 CERT: DFN-CERT-2015-1016 CERT: DFN-CERT-2015-1012 CERT: DFN-CERT-2015-0980 CERT: DFN-CERT-2015-0977 CERT: DFN-CERT-2015-0976 CERT: DFN-CERT-2015-0960 CERT: DFN-CERT-2015-0956 CERT: DFN-CERT-2015-0944 CERT: DFN-CERT-2015-0937 CERT: DFN-CERT-2015-0925 CERT: DFN-CERT-2015-0884 CERT: DFN-CERT-2015-0881 CERT: DFN-CERT-2015-0879 CERT: DFN-CERT-2015-0866 CERT: DFN-CERT-2015-0844 CERT: DFN-CERT-2015-0800 CERT: DFN-CERT-2015-0737 CERT: DFN-CERT-2015-0696 CERT: DFN-CERT-2014-0977 CERT: CB-K21/0067 CERT: CB-K19/0812 CERT: CB-K17/1750 CERT: CB-K16/1593 CERT: CB-K16/1552 CERT: CB-K16/1102 CERT: CB-K16/0617 CERT: CB-K16/0599 CERT: CB-K16/0168 CERT: CB-K16/0121 CERT: CB-K16/0090 CERT: CB-K16/0030 CERT: CB-K15/1751 CERT: CB-K15/1591 CERT: CB-K15/1550 CERT: CB-K15/1517 CERT: CB-K15/1514 CERT: CB-K15/1464 CERT: CB-K15/1442 CERT: CB-K15/1334 CERT: CB-K15/1269 CERT: CB-K15/1136 CERT: CB-K15/1090 CERT: CB-K15/1059 CERT: CB-K15/1022 CERT: CB-K15/1015 CERT: CB-K15/0986 CERT: CB-K15/0964 CERT: CB-K15/0962 CERT: CB-K15/0932 CERT: CB-K15/0927 CERT: CB-K15/0926 CERT: CB-K15/0907 CERT: CB-K15/0901 CERT: CB-K15/0896 CERT: CB-K15/0889 CERT: CB-K15/0877 CERT: CB-K15/0850 CERT: CB-K15/0849 CERT: CB-K15/0834 CERT: CB-K15/0827 CERT: CB-K15/0802 CERT: CB-K15/0764 CERT: CB-K15/0733 CERT: CB-K15/0667 CERT: CB-K14/0935 CERT: CB-K13/0942 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 40 | **Finding** | PHP 7.3.30, 7.4.x 7.4.23, 8.0.x 8.0.10 Security Update (Sep 2021) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 2021 |
| **Target** | 172.28.130.128(2021) | | |
| **Detail** | Fixed bug #81420 (ZipArchive::extractTo extracts outside of  destination). | | |
| **Solution** | Update to version 7.3.31, 7.4.24, 8.0.11 or later. | | |
| **Remark** | CVE: CVE-2021-21706 CERT: DFN-CERT-2021-2474 CERT: DFN-CERT-2021-1994 CERT: CB-K21/1008 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 41 | **Finding** | Missing `httpOnly` Cookie Attribute |
| **Severity** | **Medium** | **Port** | TCP: 2020, 2021 |
| **Target** | 172.28.130.128(2020, 2021) | | |
| **Detail** | The flaw is due to a cookie is not using the 'httpOnly' attribute. This  allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks. | | |
| **Solution** | Set the 'httpOnly' attribute for any session cookie. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 42 | **Finding** | Apache Tomcat Open Redirect Vulnerability (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** |  | | |
| **Solution** | Update to version 7.0.91, 8.5.34, 9.0.12 or later. | | |
| **Remark** | CVE: CVE-2018-11784 CERT: DFN-CERT-2019-2710 CERT: DFN-CERT-2019-2159 CERT: DFN-CERT-2019-1562 CERT: DFN-CERT-2019-1237 CERT: DFN-CERT-2019-0771 CERT: DFN-CERT-2019-0147 CERT: DFN-CERT-2019-0104 CERT: DFN-CERT-2018-2435 CERT: DFN-CERT-2018-2165 CERT: DFN-CERT-2018-2142 CERT: DFN-CERT-2018-2000 CERT: CB-K20/0029 CERT: CB-K19/1121 CERT: CB-K19/0907 CERT: CB-K19/0616 CERT: CB-K19/0320 CERT: CB-K19/0050 CERT: CB-K18/0963 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 43 | **Finding** | Apache Tomcat Session Fixation Vulnerability (Nov 2012) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | java/org/apache/catalina/authenticator/FormAuthenticator.java  in the form authentication feature does not properly handle the relationships between  authentication requirements and sessions, which allows remote attackers to inject a request into  a session by sending this request during completion of the login form, a variant of a session  fixation attack. | | |
| **Solution** | Update to version 6.0.37, 7.0.33 or later. | | |
| **Remark** | CVE: CVE-2013-2067 CERT: DFN-CERT-2014-0433 CERT: DFN-CERT-2014-0056 CERT: DFN-CERT-2013-1808 CERT: DFN-CERT-2013-1596 CERT: DFN-CERT-2013-1435 CERT: DFN-CERT-2013-1324 CERT: DFN-CERT-2013-1193 CERT: CB-K14/0417 CERT: CB-K14/0073 CERT: CB-K13/0814 CERT: CB-K13/0623 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 44 | **Finding** | Apache Tomcat XSS Vulnerability - May19 (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8081, 8443, 8444 |
| **Target** | 172.28.130.190(443, 8080, 8081, 8443, 8444) | | |
| **Detail** | The SSI printenv command in Apache Tomcat echoes user provided data without  escaping and is, therefore, vulnerable to XSS. SSI is disabled by default. The printenv command is intended for  debugging and is unlikely to be present in a production website. | | |
| **Solution** | Update to version 7.0.94, 8.5.40, 9.0.18 or later. | | |
| **Remark** | CVE: CVE-2019-0221 CERT: DFN-CERT-2021-0819 CERT: DFN-CERT-2020-1129 CERT: DFN-CERT-2020-1094 CERT: DFN-CERT-2020-0557 CERT: DFN-CERT-2019-2710 CERT: DFN-CERT-2019-2457 CERT: DFN-CERT-2019-1895 CERT: DFN-CERT-2019-1704 CERT: DFN-CERT-2019-1472 CERT: DFN-CERT-2019-1231 CERT: DFN-CERT-2019-1092 CERT: CB-K20/0029 CERT: CB-K19/0434 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 45 | **Finding** | Apache Tomcat Information Disclosure Vulnerability - Jan21 (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8081, 8443, 8444 |
| **Target** | 172.28.130.190(443, 8080, 8081, 8443, 8444) | | |
| **Detail** | When serving resources from a network location using the NTFS file system  it was possible to bypass security constraints and/or view the source code for JSPs 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. | | |
| **Solution** | Update to version 7.0.107, 8.5.60, 9.0.40, 10.0.0-M10 or later. | | |
| **Remark** | CVE: CVE-2021-24122 CERT: DFN-CERT-2021-1904 CERT: DFN-CERT-2021-0835 CERT: DFN-CERT-2021-0714 CERT: DFN-CERT-2021-0544 CERT: DFN-CERT-2021-0338 CERT: DFN-CERT-2020-2646 CERT: CB-K21/0049 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 46 | **Finding** | Apache Tomcat Security Manager Bypass Vulnerability - Feb16 (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The flaw is due to an improper validation of  'ResourceLinkFactory.setGlobalContext()' method and is accessible by web  applications running under a security manager without any checks. | | |
| **Solution** | Upgrade to version 7.0.68 or  8.0.32 or 9.0.0.M3 or later. | | |
| **Remark** | CVE: CVE-2016-0763 CERT: DFN-CERT-2017-1821 CERT: DFN-CERT-2017-0677 CERT: DFN-CERT-2017-0090 CERT: DFN-CERT-2016-1905 CERT: DFN-CERT-2016-1823 CERT: DFN-CERT-2016-1715 CERT: DFN-CERT-2016-1059 CERT: DFN-CERT-2016-0842 CERT: DFN-CERT-2016-0807 CERT: DFN-CERT-2016-0518 CERT: DFN-CERT-2016-0314 CERT: CB-K17/1750 CERT: CB-K17/0661 CERT: CB-K17/0098 CERT: CB-K16/1799 CERT: CB-K16/1758 CERT: CB-K16/1622 CERT: CB-K16/0993 CERT: CB-K16/0789 CERT: CB-K16/0758 CERT: CB-K16/0476 CERT: CB-K16/0292 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 47 | **Finding** | Apache Tomcat Parameter Handling Denial of Service Vulnerability (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The flaw is due to improper handling of large numbers of parameters  and parameter values, allows attackers to cause denial of service via a  crafted request that contains many parameters and parameter values. | | |
| **Solution** | Upgrade Apache Tomcat to 5.5.35, 6.0.34, 7.0.23 or later. | | |
| **Remark** | CVE: CVE-2012-0022 CERT: DFN-CERT-2013-1936 CERT: DFN-CERT-2012-1833 CERT: DFN-CERT-2012-1832 CERT: DFN-CERT-2012-1032 CERT: DFN-CERT-2012-0672 CERT: DFN-CERT-2012-0671 CERT: DFN-CERT-2012-0649 CERT: DFN-CERT-2012-0566 CERT: DFN-CERT-2012-0494 CERT: DFN-CERT-2012-0210 CERT: DFN-CERT-2012-0198 CERT: CB-K13/0917 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 48 | **Finding** | Apache Tomcat NIO/NIO2 Connectors Information Disclosure Vulnerability (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | The flaw exists due to an error where a  mishandling of close in 'NIO/NIO2' connectors, user sessions can get mixed up. | | |
| **Solution** | Upgrade to Apache Tomcat version 9.0.10,  8.5.32 or later. Please see the references for more information. | | |
| **Remark** | CVE: CVE-2018-8037 CERT: DFN-CERT-2019-1237 CERT: DFN-CERT-2018-2165 CERT: DFN-CERT-2018-1992 CERT: DFN-CERT-2018-1753 CERT: DFN-CERT-2018-1443 CERT: DFN-CERT-2018-1262 CERT: CB-K19/0921 CERT: CB-K18/1005 CERT: CB-K18/0809 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 49 | **Finding** | Apache Tomcat Security Constraint Incorrect Handling Access Bypass Vulnerabilities (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | Multiple flaws are due to:   - The system does not properly enforce security constraints that defined by  annotations of Servlets in certain cases, depending on the order that Servlets  are loaded.   - The URL pattern of '' (the empty string) which exactly maps to the context  root was not correctly handled when used as part of a security constraint  definition. | | |
| **Solution** | Upgrade to Apache Tomcat version 9.0.5,  8.5.28, 8.0.50, 7.0.85 or later. | | |
| **Remark** | CVE: CVE-2018-1305 CVE: CVE-2018-1304 CERT: DFN-CERT-2019-1627 CERT: DFN-CERT-2019-0772 CERT: DFN-CERT-2018-2165 CERT: DFN-CERT-2018-2142 CERT: DFN-CERT-2018-2125 CERT: DFN-CERT-2018-2103 CERT: DFN-CERT-2018-1753 CERT: DFN-CERT-2018-1407 CERT: DFN-CERT-2018-1274 CERT: DFN-CERT-2018-1253 CERT: DFN-CERT-2018-1038 CERT: DFN-CERT-2018-0922 CERT: DFN-CERT-2018-0733 CERT: DFN-CERT-2018-0455 CERT: DFN-CERT-2018-0378 CERT: CB-K19/1121 CERT: CB-K19/0321 CERT: CB-K18/1007 CERT: CB-K18/1006 CERT: CB-K18/1005 CERT: CB-K18/0790 CERT: CB-K18/0420 CERT: CB-K18/0349 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 50 | **Finding** | Apache Tomcat HTTP NIO Denial Of Service Vulnerability (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The flaw is due to error in  java/org/apache/coyote/http11/InternalNioInputBuffer.java in the HTTP NIO  connector, which does not properly restrict the request-header size. | | |
| **Solution** | Apply patch or upgrade Apache Tomcat to 6.0.36, 7.0.28 or later. | | |
| **Remark** | CVE: CVE-2012-2733 CERT: DFN-CERT-2013-1814 CERT: DFN-CERT-2013-0843 CERT: DFN-CERT-2013-0405 CERT: DFN-CERT-2013-0114 CERT: DFN-CERT-2012-2296 CERT: DFN-CERT-2012-2295 CERT: DFN-CERT-2012-2275 CERT: CB-K13/0811 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 51 | **Finding** | Apache Tomcat DoS Vulnerability (Mar 2015) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The flaw is due to ChunkedInputFilter implementation in Apache  Tomcat did not fail subsequent attempts to read input after a failure occurred. | | |
| **Solution** | Update to version 6.0.42, 7.0.55, 8.0.9 or later. | | |
| **Remark** | CVE: CVE-2014-0227 CERT: DFN-CERT-2016-0518 CERT: DFN-CERT-2015-1070 CERT: DFN-CERT-2015-0928 CERT: DFN-CERT-2015-0842 CERT: DFN-CERT-2015-0712 CERT: DFN-CERT-2015-0403 CERT: DFN-CERT-2015-0342 CERT: DFN-CERT-2015-0202 CERT: DFN-CERT-2015-0165 CERT: CB-K16/0476 CERT: CB-K15/1016 CERT: CB-K15/0874 CERT: CB-K15/0806 CERT: CB-K15/0678 CERT: CB-K15/0391 CERT: CB-K15/0330 CERT: CB-K15/0194 CERT: CB-K15/0162 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 52 | **Finding** | Apache Tomcat Multiple Security Bypass Vulnerabilities (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The flaws are due to error in HTTP digest access authentication  implementation, which does not properly validate for,   - stale nonce values in conjunction with enforcement of proper credentials   - caches information about the authenticated user within the session state   - cnonce values instead of nonce and nc values. | | |
| **Solution** | Apply patch or upgrade Apache Tomcat to 5.5.36, 6.0.36, 7.0.30 or later. | | |
| **Remark** | CVE: CVE-2012-5887 CVE: CVE-2012-5886 CVE: CVE-2012-5885 CERT: DFN-CERT-2013-1936 CERT: DFN-CERT-2013-1814 CERT: DFN-CERT-2013-1008 CERT: DFN-CERT-2013-0843 CERT: DFN-CERT-2013-0545 CERT: DFN-CERT-2013-0523 CERT: DFN-CERT-2013-0405 CERT: DFN-CERT-2013-0114 CERT: DFN-CERT-2012-2296 CERT: DFN-CERT-2012-2295 CERT: CB-K13/0917 CERT: CB-K13/0811 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 53 | **Finding** | Apache Tomcat Request Object Security Bypass Vulnerability (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The flaw is due to improper recycling of the request object before  processing the next request when logging certain actions, allowing attackers  to gain sensitive information like remote IP address and HTTP headers which  is being carried forward to the next request. | | |
| **Solution** | Upgrade Apache Tomcat to 6.0.34, 7.0.22 or later. | | |
| **Remark** | CVE: CVE-2011-3375 CERT: DFN-CERT-2012-1833 CERT: DFN-CERT-2012-0627 CERT: DFN-CERT-2012-0494 CERT: DFN-CERT-2012-0198 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 54 | **Finding** | Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | Multiple flaws exist due to:   - An error in the system property replacement feature for configuration files.   - An error in the realm implementations in Apache Tomcat that does not process  the supplied password if the supplied user name did not exist.   - An error in the configured SecurityManager via a Tomcat utility method that  is accessible to web applications.   - An error in the configured SecurityManager via manipulation of the  configuration parameters for the JSP Servlet.   - An error in the ResourceLinkFactory implementation in Apache Tomcat that  does not limit web application access to global JNDI resources to those  resources explicitly linked to the web application. | | |
| **Solution** | Upgrade to Apache Tomcat version 9.0.0.M10  or 8.5.5 or 8.0.37 or 7.0.72 or 6.0.47 or later. | | |
| **Remark** | CVE: CVE-2016-6794 CVE: CVE-2016-0762 CVE: CVE-2016-5018 CVE: CVE-2016-6796 CVE: CVE-2016-6797 CERT: DFN-CERT-2017-1095 CERT: DFN-CERT-2017-1068 CERT: DFN-CERT-2017-1064 CERT: DFN-CERT-2017-0673 CERT: DFN-CERT-2017-0404 CERT: DFN-CERT-2017-0137 CERT: DFN-CERT-2016-2035 CERT: DFN-CERT-2016-1772 CERT: DFN-CERT-2016-1743 CERT: CB-K17/1060 CERT: CB-K17/1033 CERT: CB-K17/1031 CERT: CB-K17/0659 CERT: CB-K17/0397 CERT: CB-K17/0133 CERT: CB-K16/1927 CERT: CB-K16/1673 CERT: CB-K16/1646 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 55 | **Finding** | Apache Tomcat Denial Of Service Vulnerability (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | Flaw due to improper validation of an error in the way CRLF sequences at the  end of data chunks are processed by chunked transfer encoding. | | |
| **Solution** | Apply patch or upgrade Apache Tomcat to 7.0.30 or 6.0.38 or later. | | |
| **Remark** | CVE: CVE-2012-3544 CERT: DFN-CERT-2014-1111 CERT: DFN-CERT-2014-0917 CERT: DFN-CERT-2014-0056 CERT: DFN-CERT-2014-0049 CERT: DFN-CERT-2013-1596 CERT: DFN-CERT-2013-1435 CERT: DFN-CERT-2013-1324 CERT: CB-K14/1067 CERT: CB-K14/0876 CERT: CB-K14/0073 CERT: CB-K14/0058 CERT: CB-K13/0623 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 56 | **Finding** | Apache Tomcat SecurityManager Security Bypass Vulnerability - Jun15 (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The flaw is due to the Expression Language  does not properly consider the possibility of an accessible interface  implemented by an inaccessible class. | | |
| **Solution** | Upgrade to version 6.0.44 or 7.0.58 or  8.0.16 or later. | | |
| **Remark** | CVE: CVE-2014-7810 CERT: DFN-CERT-2019-0735 CERT: DFN-CERT-2019-0646 CERT: DFN-CERT-2018-2077 CERT: DFN-CERT-2016-1726 CERT: DFN-CERT-2016-1661 CERT: DFN-CERT-2016-0537 CERT: DFN-CERT-2016-0518 CERT: DFN-CERT-2016-0494 CERT: DFN-CERT-2016-0042 CERT: DFN-CERT-2015-1632 CERT: DFN-CERT-2015-1251 CERT: DFN-CERT-2015-0928 CERT: DFN-CERT-2015-0703 CERT: CB-K16/1630 CERT: CB-K16/1568 CERT: CB-K16/0496 CERT: CB-K16/0476 CERT: CB-K16/0455 CERT: CB-K16/0034 CERT: CB-K15/1550 CERT: CB-K15/1182 CERT: CB-K15/0874 CERT: CB-K15/0679 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 57 | **Finding** | SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability |
| **Severity** | **Medium** | **Port** | TCP: 3389, 8443 |
| **Target** | 172.28.130.190(8443), 172.28.190.139(3389) | | |
| **Detail** | The Diffie-Hellman group are some big numbers that are used as base for  the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size  of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really  powerful attackers like governments. | | |
| **Solution** | Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use  a 2048-bit or stronger Diffie-Hellman group (see the references).   For Apache Web Servers:  Beginning with version 2.4.7, mod\_ssl will use DH parameters which include primes with lengths of more than 1024 bits. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 58 | **Finding** | Apache Tomcat Limited Directory Traversal Vulnerability - Feb16 (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The flaw is due to an improper validation of  path while accessing resources via the ServletContext methods getResource(),  getResourceAsStream() and getResourcePaths() the paths should be limited to  the current web application. | | |
| **Solution** | Upgrade to version 6.0.45 or 7.0.65 or  8.0.27 or later. | | |
| **Remark** | CVE: CVE-2015-5174 CERT: DFN-CERT-2018-0077 CERT: DFN-CERT-2016-1823 CERT: DFN-CERT-2016-1726 CERT: DFN-CERT-2016-1661 CERT: DFN-CERT-2016-1161 CERT: DFN-CERT-2016-1059 CERT: DFN-CERT-2016-0842 CERT: DFN-CERT-2016-0635 CERT: DFN-CERT-2016-0537 CERT: DFN-CERT-2016-0518 CERT: DFN-CERT-2016-0314 CERT: DFN-CERT-2015-1950 CERT: CB-K18/0066 CERT: CB-K16/1758 CERT: CB-K16/1630 CERT: CB-K16/1568 CERT: CB-K16/1089 CERT: CB-K16/0993 CERT: CB-K16/0789 CERT: CB-K16/0587 CERT: CB-K16/0496 CERT: CB-K16/0476 CERT: CB-K16/0292 CERT: CB-K15/1841 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 59 | **Finding** | Apache Tomcat JNDI Realm Authentication Weakness Vulnerability (Jul 2021) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8081, 8443, 8444 |
| **Target** | 172.28.130.190(443, 8080, 8081, 8443, 8444) | | |
| **Detail** | Queries made by the JNDI Realm do 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 is possible for  users to authenticate using variations of their user name and/or to bypass some of the protection  provided by the LockOut Realm. | | |
| **Solution** | Update to version 7.0.109, 8.5.66, 9.0.46, 10.0.6 or later. | | |
| **Remark** | CVE: CVE-2021-30640 CERT: DFN-CERT-2021-2496 CERT: DFN-CERT-2021-2438 CERT: DFN-CERT-2021-2297 CERT: DFN-CERT-2021-2169 CERT: DFN-CERT-2021-1728 CERT: DFN-CERT-2021-1668 CERT: DFN-CERT-2021-1472 CERT: CB-K21/0733 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 60 | **Finding** | Apache Tomcat Hash Collision Denial Of Service Vulnerability |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The flaw is due to an error within a hash generation function when  computing hash values for form parameter and updating a hash table. This can  be exploited to cause a hash collision resulting in high CPU consumption via  a specially crafted form sent in a HTTP POST request. | | |
| **Solution** | Apply patch or upgrade Apache Tomcat to 5.5.35, 6.0.35, 7.0.23 or later. | | |
| **Remark** | CVE: CVE-2011-4858 CERT: DFN-CERT-2012-1833 CERT: DFN-CERT-2012-1832 CERT: DFN-CERT-2012-1032 CERT: DFN-CERT-2012-0863 CERT: DFN-CERT-2012-0672 CERT: DFN-CERT-2012-0671 CERT: DFN-CERT-2012-0649 CERT: DFN-CERT-2012-0566 CERT: DFN-CERT-2012-0210 CERT: DFN-CERT-2012-0198 CERT: DFN-CERT-2012-0110 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 61 | **Finding** | Apache Tomcat HTTP/2 Vulnerability - Oct20 (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | If an HTTP/2 client exceeded 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 could lead to users seeing responses for unexpected resources. | | |
| **Solution** | Update to version 8.5.58, 9.0.38, 10.0.0-M8 or later. | | |
| **Remark** | CVE: CVE-2020-13943 CERT: DFN-CERT-2021-2620 CERT: DFN-CERT-2021-0338 CERT: DFN-CERT-2021-0134 CERT: DFN-CERT-2021-0034 CERT: DFN-CERT-2020-2224 CERT: CB-K20/0971 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 62 | **Finding** | Apache Tomcat HTTP Request Smuggling Vulnerability (Jul 2021) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **Detail** | Apache Tomcat does 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 ignores the transfer-encoding header if  the client declared it would only accept an HTTP/1.0 response. Tomcat honours the identify  encoding and Tomcat does not ensure that, if present, the chunked encoding is the final encoding. | | |
| **Solution** | Update to version 8.5.68, 9.0.48, 10.0.7 or later. | | |
| **Remark** | CVE: CVE-2021-33037 CERT: DFN-CERT-2021-2496 CERT: DFN-CERT-2021-2297 CERT: DFN-CERT-2021-2223 CERT: DFN-CERT-2021-2193 CERT: DFN-CERT-2021-2188 CERT: DFN-CERT-2021-1728 CERT: DFN-CERT-2021-1668 CERT: DFN-CERT-2021-1472 CERT: CB-K22/0066 CERT: CB-K21/1087 CERT: CB-K21/1084 CERT: CB-K21/0733 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 63 | **Finding** | Apache Tomcat Directory Disclosure Vulnerability - Feb16 (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The flaw is due to an improper accessing a  directory protected by a security constraint with a URL that did not end in  a slash. | | |
| **Solution** | Upgrade to version 6.0.45 or 7.0.67 or  8.0.30 or 9.0.0.M3 later. | | |
| **Remark** | CVE: CVE-2015-5345 CERT: DFN-CERT-2016-1823 CERT: DFN-CERT-2016-1726 CERT: DFN-CERT-2016-1661 CERT: DFN-CERT-2016-1059 CERT: DFN-CERT-2016-0842 CERT: DFN-CERT-2016-0807 CERT: DFN-CERT-2016-0537 CERT: DFN-CERT-2016-0518 CERT: DFN-CERT-2016-0314 CERT: CB-K16/1758 CERT: CB-K16/1630 CERT: CB-K16/1568 CERT: CB-K16/0993 CERT: CB-K16/0789 CERT: CB-K16/0758 CERT: CB-K16/0496 CERT: CB-K16/0476 CERT: CB-K16/0292 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 64 | **Finding** | SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits |
| **Severity** | **Medium** | **Port** | TCP: 8443 |
| **Target** | 172.28.130.190(8443) | | |
| **Detail** | SSL/TLS certificates using RSA keys with less than 2048 bits are  considered unsafe. | | |
| **Solution** | Replace the certificate with a stronger key and reissue the  certificates it signed. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 65 | **Finding** | SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) |
| **Severity** | **Medium** | **Port** | TCP: 3978, 5007, 8443 |
| **Target** | 172.28.130.190(8443), 172.28.188.168(3978, 5007) | | |
| **Detail** | The flaw exists because the remote SSL/TLS service does not  properly restrict client-initiated renegotiation within the SSL and TLS protocols.   Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but  both are in a DISPUTED state with the following rationale:   > It can also be argued that it is the responsibility of server deployments, not a security  library, to prevent or limit renegotiation when it is inappropriate within a specific environment.   Both CVEs are still kept in this VT as a reference to the origin of this flaw. | | |
| **Solution** | Users should contact their vendors for specific patch information.   A general solution is to remove/disable renegotiation capabilities altogether from/in the affected  SSL/TLS service. | | |
| **Remark** | CVE: CVE-2011-1473 CVE: CVE-2011-5094 CERT: DFN-CERT-2017-1013 CERT: DFN-CERT-2017-1012 CERT: DFN-CERT-2014-0809 CERT: DFN-CERT-2013-1928 CERT: DFN-CERT-2012-1112 CERT: CB-K17/0980 CERT: CB-K17/0979 CERT: CB-K14/0772 CERT: CB-K13/0915 CERT: CB-K13/0462 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 66 | **Finding** | SSL/TLS: Certificate Expired |
| **Severity** | **Medium** | **Port** | TCP: 8444 |
| **Target** | 172.28.130.190(8444) | | |
| **Detail** | This script checks expiry dates of certificates associated with  SSL/TLS-enabled services on the target and reports whether any have already expired. | | |
| **Solution** | Replace the SSL/TLS certificate by a new one. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 67 | **Finding** | SSL/TLS: Certificate Signed Using A Weak Signature Algorithm |
| **Severity** | **Medium** | **Port** | TCP: 8443 |
| **Target** | 172.28.130.190(8443) | | |
| **Detail** | The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak  and not secure enough for ongoing use:   - Secure Hash Algorithm 1 (SHA-1)   - Message Digest 5 (MD5)   - Message Digest 4 (MD4)   - Message Digest 2 (MD2)   Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting  web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.   NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints  needs to be passed comma-separated and case-insensitive:   Fingerprint1   or   fingerprint1, Fingerprint2 | | |
| **Solution** | Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new  SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 68 | **Finding** | Apache Tomcat ServletSecurity Annotations Security Bypass Vulnerability (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | The flaw is due to when a web application  was started, ServletSecurity annotations were ignored. This meant that some  areas of the application may not have been protected as expected. | | |
| **Solution** | Upgrade to Tomcat version 7.0.11 or later. | | |
| **Remark** | CVE: CVE-2011-1088 CVE: CVE-2011-1419 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 69 | **Finding** | SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection |
| **Severity** | **Medium** | **Port** | TCP: 443, 3978 |
| **Target** | 172.28.188.167(443), 172.28.188.168(443, 3978) | | |
| **Detail** |  | | |
| **Solution** | Replace the SSL/TLS certificate with one signed by a trusted  CA. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 70 | **Finding** | Weak Encryption Algorithm(s) Supported (SSH) |
| **Severity** | **Medium** | **Port** | TCP: 22 |
| **Target** | 172.28.188.167(22), 172.28.188.168(22) | | |
| **Detail** | '- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit  keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour  (and RC4) has problems with weak keys, and should not be used anymore.   - The 'none' algorithm specifies that no encryption is to be done. Note that this method provides  no confidentiality protection, and it is NOT RECOMMENDED to use it.   - A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to  recover plaintext from a block of ciphertext. | | |
| **Solution** | Disable the reported weak encryption algorithm(s). | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 71 | **Finding** | Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) |
| **Severity** | **Medium** | **Port** | TCP: 22 |
| **Target** | 172.28.188.167(22), 172.28.188.168(22) | | |
| **Detail** | '- 1024-bit MODP group / prime KEX algorithms:   Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key  exchange. Practitioners believed this was safe as long as new key exchange messages were generated  for every connection. However, the first step in the number field sieve-the most efficient  algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.   A nation-state can break a 1024-bit prime. | | |
| **Solution** | Disable the reported weak KEX algorithm(s)   - 1024-bit MODP group / prime KEX algorithms:   Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 72 | **Finding** | TCP timestamps |
| **Severity** | **Low** | **Port** | TCP: 0 |
| **Target** | 172.28.130.128(0), 172.28.130.190(0), 172.28.135.188(0), 172.28.135.189(0), 172.28.188.167(0), 172.28.188.168(0), 172.28.190.139(0) | | |
| **Detail** | The remote host implements TCP timestamps, as defined by RFC1323/RFC7323. | | |
| **Solution** | To disable TCP timestamps on linux add the line 'net.ipv4.tcp\_timestamps = 0' to  /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.   To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'   Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.   The default behavior of the TCP/IP stack on this Systems is to not use the  Timestamp options when initiating TCP connections, but use them if the TCP peer  that is initiating communication includes them in their synchronize (SYN) segment.   See the references for more information. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 73 | **Finding** | Apache Tomcat Information Disclosure Vulnerability (May 2013) - Windows |
| **Severity** | **Low** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **Detail** | java/org/apache/catalina/core/AsyncContextImpl.java does not  properly handle the throwing of a RuntimeException in an AsyncListener in an application, which  allows context-dependent attackers to obtain sensitive request information intended for other  applications in opportunistic circumstances via an application that records the requests that it  processes. | | |
| **Solution** | Update to version 7.0.40 or later. | | |
| **Remark** | CVE: CVE-2013-2071 CERT: DFN-CERT-2014-0433 CERT: DFN-CERT-2014-0056 CERT: DFN-CERT-2013-1436 CERT: DFN-CERT-2013-0928 CERT: CB-K14/0417 CERT: CB-K14/0073 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 74 | **Finding** | Weak MAC Algorithm(s) Supported (SSH) |
| **Severity** | **Low** | **Port** | TCP: 22 |
| **Target** | 172.28.188.167(22), 172.28.188.168(22) | | |
| **Detail** |  | | |
| **Solution** | Disable the reported weak MAC algorithm(s). | | |
| **Remark** |  | | |



# Appendix

## **6.1 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

### **6.1.1 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

### **6.1.2 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 |

## **6.2 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

### **6.2.1 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. |