**Vulnerability Assessment Report**

**For**



**SIPH-greenbone**

**May 03, 2022**

**Document Security Level:** Confidential

**Document Version:** 1.0

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Edit Report** | **Editor** |
| 1.0 | May 03, 2022 | Creation | INET Managed Services |

|  |  |  |  |
| --- | --- | --- | --- |
| SIPH-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](#_Toc100647613)

[2. Operation Method 5](#_Toc100647614)

[3. Project Scope 6](#_Toc100647615)

[3.1 Infrastructure Vulnerability Assessment 6](#_Toc100647616)

[4. Testing Tools 7](#_Toc100647617)

[5. Infrastructure Vulnerability Assessment 7](#_Toc100647618)

[5.1 Target Information 8](#_Toc100647619)

[5.2 Executive summary 9](#_Toc100647620)

[5.2.1 Summary Vulnerability by Severity 9](#_Toc100647621)

[5.2.2 Vulnerability by Target 9](#_Toc100647622)

[5.3 Infrastructure Vulnerability Detail 10](#_Toc100647623)

[6 Port Discovery 11](#_Toc100647624)

[7. Appendix 12](#_Toc100647625)

[7.1 About Nessus 12](#_Toc100647626)

[7.1.1 Nessus vulnerabilities 12](#_Toc100647627)

[7.1.2 Nessus risk score 12](#_Toc100647628)

# 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 |
| Greenbone | Infrastructure 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 | - | 172.28.131.23 | - | TCP : 22, 80, 427, 443, 902, 5988, 5989, 8000, 8300, 9080 |
| 2 | - | 172.28.131.24 | - | TCP : 22, 80, 443, 3011, 3031, 5432, 8080, 8090, 9090, 9200 |
| 3 | - | 172.28.131.48 | - | TCP : 135, 139, 445, 3389 |
| 4 | - | 172.28.131.49 | - | TCP : 135, 139, 445, 3306, 3389, 4848, 8080, 8181, 10001 |
| 5 | - | 172.28.131.102 | - | TCP : 135, 139, 443, 445, 3389, 4000, 6001, 6101, 7000, 27000, 49152, 49153, 49154, 50002 |
| 6 | - | 172.28.131.105 | - | TCP : 80, 135, 139, 445, 1007, 1010, 1011, 1433, 2007, 3389, 4045, 9998, 49152, 49153, 49154 |
| 7 | - | 172.28.131.108 | - | TCP : 135, 139, 445, 3389, 49152, 49153, 49154, 49155 |
| 8 | - | 172.28.135.223 | - | TCP : 80, 135, 139, 445, 3389, 5800, 5900, 49152, 49153, 49154, 49155, 49156 |
| 9 | - | 172.28.136.118 | - | TCP : 135, 139, 445, 1433, 3211, 3389, 65000 |
| 10 | - | 172.28.136.153 | - | TCP : 80, 135, 139, 443, 445, 3389, 49152, 49153, 49154, 49155, 49167 |
| 11 | - | 172.28.137.52 | - | TCP : 22, 111, 1556, 3211, 3301, 6001, 8000, 8001, 8081, 13782 |
| 12 | - | 172.28.140.41 | - | TCP : 22, 80, 427, 443, 902, 5988, 5989, 8000, 8300, 9080 |
| 13 | - | 172.28.140.43 | - | TCP : 22, 9000 |
| 14 | - | 172.28.140.45 | - | TCP : 22, 81, 443, 8080, 9000 |
| 15 | - | 172.28.190.131 | - | TCP : 135, 139, 445, 3389, 49152, 49153, 49154, 49155, 49157, 49167 |
| 16 | - | 172.28.190.133 | - | TCP : 80, 135, 139, 443, 445, 3389, 49152, 49153, 49154, 49155, 49159, 65000 |

## **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**

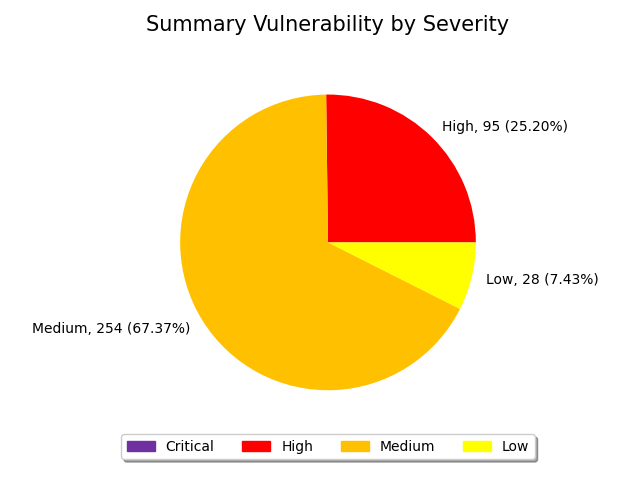


Figure 4: Summary by Severity of Infrastructure Vulnerability Assessment

### **5.2.2 Vulnerability by Target**

| **No.** | **Domain/Server Name** | **IP Address** | **Critical** | **High** | **Medium** | **Low** | **Total** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | - | 172.28.130.33 | 0 | 0 | 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 | - | 172.28.131.23 | 0 | 0 | 7 | 1 | 8 |
| 7 | - | 172.28.131.24 | 0 | 1 | 17 | 2 | 20 |
| 8 | - | 172.28.131.48 | 0 | 0 | 2 | 1 | 3 |
| 9 | - | 172.28.131.49 | 0 | 1 | 7 | 0 | 8 |
| 10 | - | 172.28.131.102 | 0 | 0 | 9 | 1 | 10 |
| 11 | - | 172.28.131.105 | 0 | 0 | 4 | 1 | 5 |
| 12 | - | 172.28.131.108 | 0 | 8 | 28 | 3 | 39 |
| 13 | - | 172.28.135.188 | 0 | 0 | 0 | 1 | 1 |
| 14 | - | 172.28.135.189 | 0 | 0 | 2 | 1 | 3 |
| 15 | - | 172.28.135.223 | 0 | 0 | 5 | 1 | 6 |
| 16 | - | 172.28.136.111 | 0 | 0 | 5 | 1 | 6 |
| 17 | - | 172.28.136.118 | 0 | 0 | 3 | 1 | 4 |
| 18 | - | 172.28.136.141 | 0 | 0 | 3 | 0 | 3 |
| 19 | - | 172.28.136.153 | 0 | 1 | 4 | 1 | 6 |
| 20 | - | 172.28.137.52 | 0 | 0 | 6 | 0 | 6 |
| 21 | - | 172.28.137.112 | 0 | 2 | 12 | 1 | 15 |
| 22 | - | 172.28.188.167 | 0 | 1 | 5 | 2 | 8 |
| 23 | - | 172.28.188.168 | 0 | 1 | 9 | 2 | 12 |
| 24 | - | 172.28.190.131 | 0 | 0 | 4 | 1 | 5 |
| 25 | - | 172.28.190.133 | 0 | 0 | 6 | 1 | 7 |
| 26 | - | 172.28.190.139 | 0 | 0 | 3 | 1 | 4 |
| 27 | - | 172.28.190.153 | 0 | 0 | 3 | 0 | 3 |
| **Total** | | | 0 | 95 | 254 | 28 | 377 |

## **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) | | |
| **CVS 3.0**  **Score** | 9.8 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 2 | **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) | | |
| **CVS 3.0**  **Score** | 7.0 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 3 | **Finding** | PHP CVE-2017-7189 Improper Input Validation Vulnerability (Windows) |
| **Severity** | **High** | **Port** | TCP: 2021 |
| **Target** | 172.28.130.128(2021) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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.** | 4 | **Finding** | Apache Tomcat DoS Vulnerability (Apr 2014) - Windows |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 5 | **Finding** | Apache Tomcat DoS Vulnerability - June20 (Windows) |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 6 | **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) | | |
| **CVS 3.0**  **Score** | 7.1 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 7 | **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) | | |
| **CVS 3.0**  **Score** | 7.0 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 8 | **Finding** | Apache Tomcat pipelined Requests Information Disclosure Vulnerability (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 9 | **Finding** | Apache Tomcat DoS Vulnerability (Sep 2021) - Windows |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 10 | **Finding** | Apache Tomcat DoS Vulnerability - June19 (Windows) |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 11 | **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) | | |
| **CVS 3.0**  **Score** | 7.0 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 12 | **Finding** | Apache Tomcat Multiple DoS Vulnerabilities - July20 (Windows) |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 13 | **Finding** | Apache Tomcat DoS Vulnerability - June19 (Windows) |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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 8.5.41, 9.0.20 or later. | | |
| **Remark** | CVE: CVE-2019-10072 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 14 | **Finding** | Apache Tomcat SecurityManager Information Disclosure Vulnerability (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 9.1 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 15 | **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) | | |
| **CVS 3.0**  **Score** | 7.0 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 16 | **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) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 17 | **Finding** | Apache Tomcat HTTP/2 Vulnerability - Dec20 (Windows) |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 18 | **Finding** | Apache Tomcat DoS Vulnerability - March19 (Windows) |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 19 | **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) | | |
| **CVS 3.0**  **Score** | 9.8 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 20 | **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) | | |
| **CVS 3.0**  **Score** | 8.1 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 21 | **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) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 22 | **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) | | |
| **CVS 3.0**  **Score** | 8.8 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 23 | **Finding** | Apache Tomcat Security Bypass Vulnerability (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 24 | **Finding** | Apache Tomcat Hostname Verification Security Bypass Vulnerability (Windows) |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 25 | **Finding** | Apache Tomcat AJP RCE Vulnerability (Ghostcat) |
| **Severity** | **High** | **Port** | TCP: 8009 |
| **Target** | 172.28.130.190(8009) | | |
| **CVS 3.0**  **Score** | 9.8 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 26 | **Finding** | Apache Tomcat VirtualDirContext Information Disclosure Vulnerability (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 27 | **Finding** | Apache Tomcat Information Disclosure Vulnerability (Mar21) - Windows |
| **Severity** | **High** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 28 | **Finding** | Apache Tomcat Denial Of Service Vulnerability - Jun15 (Windows) |
| **Severity** | **High** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 7.8 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 29 | **Finding** | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS |
| **Severity** | **High** | **Port** | TCP: 443, 8443, 10102 |
| **Target** | 172.28.130.190(8443), 172.28.131.49(10102), 172.28.136.153(443), 172.28.188.167(443), 172.28.188.168(443) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 30 | **Finding** | SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability |
| **Severity** | **High** | **Port** | TCP: 3031 |
| **Target** | 172.28.131.24(3031) | | |
| **CVS 3.0**  **Score** | 7.4 | | |
| **Detail** | OpenSSL does not properly restrict processing of ChangeCipherSpec  messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in  certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive  information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability. | | |
| **Solution** | Updates are available. Please see the references for more information. | | |
| **Remark** | CVE: CVE-2014-0224 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 31 | **Finding** | Oracle Mysql Security Update (cpuoct2018 - 02) - Windows |
| **Severity** | **High** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 9.8 | | |
| **Detail** | Multiple flaws exist due to:  - An unspecified error within 'InnoDB (zlib)' component of MySQL Server.  - An unspecified error within 'Server: Parser' component of MySQL Server.  - An unspecified error within 'Client programs' component of MySQL Server.  - An unspecified error within 'Server: Storage Engines' component of MySQL Server. | | |
| **Solution** | The vendor has released updates. Please see the references for  more information. | | |
| **Remark** | CVE: CVE-2018-3133 CVE: CVE-2018-3174 CVE: CVE-2018-3282 CVE: CVE-2016-9843 CVE: CVE-2016-9840 CVE: CVE-2016-9841 CVE: CVE-2016-9842 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 32 | **Finding** | Oracle Mysql Security Updates (jan2018-3236628) 04 - Windows |
| **Severity** | **High** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 7.1 | | |
| **Detail** | The flaw exists due to an error in  'Server:Partition' component. | | |
| **Solution** | Apply the patch from the referenced advisory. | | |
| **Remark** | CVE: CVE-2018-2562 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 33 | **Finding** | Oracle MySQL Server = 5.6.42 / 5.7 = 5.7.24 / 8.0 = 8.0.13 Security Update (cpujan2019) - Windows |
| **Severity** | **High** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 7.1 | | |
| **Detail** | The attacks range in variety and difficulty. Most of them allow an attacker  with network access via multiple protocols to compromise the MySQL Server.  For further information refer to the official advisory via the referenced link. | | |
| **Solution** | Updates are available. Apply the necessary patch from the referenced link. | | |
| **Remark** | CVE: CVE-2019-2534 CVE: CVE-2019-2529 CVE: CVE-2019-2482 CVE: CVE-2019-2455 CVE: CVE-2019-2503 CVE: CVE-2018-0734 CVE: CVE-2019-2537 CVE: CVE-2019-2481 CVE: CVE-2019-2507 CVE: CVE-2019-2531 CVE: CVE-2018-5407 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 34 | **Finding** | Oracle MySQL Server = 5.6.48 Security Update (cpujul2020) - Windows |
| **Severity** | **High** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **Detail** | None | | |
| **Solution** | Update to version 5.6.49 or later. | | |
| **Remark** | CVE: CVE-2020-1967 CVE: CVE-2020-14539 CVE: CVE-2020-14559 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 35 | **Finding** | Oracle MySQL Server = 5.7.35 / 8.0 = 8.0.26 Security Update (cpuoct2021) - Windows |
| **Severity** | **High** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 9.8 | | |
| **Detail** | None | | |
| **Solution** | Update to version 5.7.36, 8.0.27 or later. | | |
| **Remark** | CVE: CVE-2021-3711 CVE: CVE-2021-22926 CVE: CVE-2021-35604 CVE: CVE-2021-35624 CVE: CVE-2021-22922 CVE: CVE-2021-22923 CVE: CVE-2021-22924 CVE: CVE-2021-22925 CVE: CVE-2021-22945 CVE: CVE-2021-22946 CVE: CVE-2021-22947 CVE: CVE-2021-3712 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 36 | **Finding** | Oracle MySQL Denial Of Service Vulnerability Feb17 (Windows) |
| **Severity** | **High** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **Detail** | Multiple errors exist as,  - In sql-common/client.c script 'mysql\_prune\_stmt\_list' function, the for loop  adds elements to pruned\_list without removing it from the existing list.  - If application gets disconnected just before it tries to prepare a new  statement, 'mysql\_prune\_stmt\_list' tries to detach all previously prepared  statements. | | |
| **Solution** | Upgrade to Oracle MySQL version 5.6.21 or  5.7.5 or later. | | |
| **Remark** | CVE: CVE-2017-3302 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 37 | **Finding** | Oracle MySQL Server = 5.7.33 / 8.0 = 8.0.23 Security Update (cpuapr2021) - Windows |
| **Severity** | **High** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 7.4 | | |
| **Detail** | None | | |
| **Solution** | Update to version 5.7.34, 8.0.24 or later. | | |
| **Remark** | CVE: CVE-2021-3449 CVE: CVE-2021-3450 CVE: CVE-2021-23840 CVE: CVE-2021-23841 CVE: CVE-2021-2307 CVE: CVE-2021-2304 CVE: CVE-2021-2180 CVE: CVE-2021-2194 CVE: CVE-2021-2166 CVE: CVE-2021-2179 CVE: CVE-2021-2226 CVE: CVE-2021-2169 CVE: CVE-2021-2146 CVE: CVE-2021-2174 CVE: CVE-2021-2171 CVE: CVE-2021-2162 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 38 | **Finding** | Oracle MySQL Server = 5.7.29 / 8.0 = 8.0.19 Security Update (cpuapr2021) - Windows |
| **Severity** | **High** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 7.2 | | |
| **Detail** | None | | |
| **Solution** | Update to version 5.7.30, 8.0.20 or later. | | |
| **Remark** | CVE: CVE-2021-2144 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 39 | **Finding** | OpenSSH Multiple Vulnerabilities Jan17 (Windows) |
| **Severity** | **High** | **Port** | TCP: 22 |
| **Target** | 172.28.137.112(22) | | |
| **CVS 3.0**  **Score** | 7.3 | | |
| **Detail** | Multiple flaws exist due to:  - An 'authfile.c' script does not properly consider the effects of realloc  on buffer contents.  - The shared memory manager (associated with pre-authentication compression)  does not ensure that a bounds check is enforced by all compilers.  - The sshd in OpenSSH creates forwarded Unix-domain sockets as root, when  privilege separation is not used.  - An untrusted search path vulnerability in ssh-agent.c in ssh-agent.  - NULL pointer dereference error due to an out-of-sequence NEWKEYS message. | | |
| **Solution** | Upgrade to OpenSSH version 7.4 or later. | | |
| **Remark** | CVE: CVE-2016-10009 CVE: CVE-2016-10010 CVE: CVE-2016-10011 CVE: CVE-2016-10012 CVE: CVE-2016-10708 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 40 | **Finding** | OpenSSH Denial of Service And User Enumeration Vulnerabilities (Windows) |
| **Severity** | **High** | **Port** | TCP: 22 |
| **Target** | 172.28.137.112(22) | | |
| **CVS 3.0**  **Score** | 7.5 | | |
| **Detail** | Multiple flaws exist due to:  - The auth\_password function in 'auth-passwd.c' script does not limit password  lengths for password authentication.  - The sshd in OpenSSH, when SHA256 or SHA512 are used for user password hashing  uses BLOWFISH hashing on a static password when the username does not exist  and it takes much longer to calculate SHA256/SHA512 hash than BLOWFISH hash. | | |
| **Solution** | Upgrade to OpenSSH version 7.3 or later. | | |
| **Remark** | CVE: CVE-2016-6515 CVE: CVE-2016-6210 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 41 | **Finding** | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection |
| **Severity** | **Medium** | **Port** | TCP: 443, 636, 1129, 3031, 3269, 3389, 3978, 4300, 4316, 5989, 6101, 6301, 7630, 8443, 8444, 9080, 10102 |
| **Target** | 172.28.130.33(636, 3269, 3389), 172.28.130.128(3389), 172.28.130.190(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, 6101, 6301), 172.28.131.105(3389, 8444), 172.28.131.108(3389), 172.28.135.189(3389), 172.28.135.223(3389), 172.28.136.111(1129, 3389), 172.28.136.118(1129, 3389), 172.28.136.141(1129, 3389), 172.28.136.153(443, 3389), 172.28.137.52(1129, 4300), 172.28.137.112(1129, 4316, 7630), 172.28.188.167(443), 172.28.188.168(443, 3978), 172.28.190.131(3389), 172.28.190.133(443, 1129, 3389), 172.28.190.139(3389), 172.28.190.153(443, 3389) | | |
| **CVS 3.0**  **Score** | 4.3 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 42 | **Finding** | Cleartext Transmission of Sensitive Information via HTTP |
| **Severity** | **Medium** | **Port** | TCP: 80, 2021, 4848, 6161, 8001, 8080, 9200 |
| **Target** | 172.28.130.33(6161), 172.28.130.35(80), 172.28.130.128(2021), 172.28.130.190(8080), 172.28.131.24(9200), 172.28.131.49(4848), 172.28.137.52(8001) | | |
| **CVS 3.0**  **Score** | 4.8 | | |
| **Detail** | None | | |
| **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.** | 43 | **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), 172.28.131.48(135), 172.28.131.49(135), 172.28.131.102(135), 172.28.131.105(135), 172.28.131.108(135), 172.28.135.189(135), 172.28.135.223(135), 172.28.136.111(135), 172.28.136.118(135), 172.28.136.141(135), 172.28.136.153(135), 172.28.190.131(135), 172.28.190.133(135), 172.28.190.153(135) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **Detail** | None | | |
| **Solution** | Filter incoming traffic to this ports. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 44 | **Finding** | SMTP Server on non standard port |
| **Severity** | **Medium** | **Port** | TCP: 475, 476, 477, 2525, 25000 |
| **Target** | 172.28.130.35(475, 476, 477, 2525), 172.28.130.37(475, 476, 477, 2525), 172.28.137.52(25000) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **Detail** | None | | |
| **Solution** | Check and clean your configuration. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 45 | **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) | | |
| **CVS 3.0**  **Score** | 5.3 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 46 | **Finding** | Sensitive File Disclosure (HTTP) |
| **Severity** | **Medium** | **Port** | TCP: 2020 |
| **Target** | 172.28.130.128(2020) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **Detail** | None | | |
| **Solution** | The sensitive files shouldn't be accessible via a web server.  Restrict access to it or remove it completely. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 47 | **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) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **Detail** | None | | |
| **Solution** | Update to version 7.3.30, 7.4.23, 8.0.10 or later. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 48 | **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) | | |
| **CVS 3.0**  **Score** | 6.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 49 | **Finding** | Missing `httpOnly` Cookie Attribute |
| **Severity** | **Medium** | **Port** | TCP: 2020, 2021, 7630, 8081 |
| **Target** | 172.28.130.128(2020, 2021), 172.28.137.52(8081), 172.28.137.112(7630) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **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.** | 50 | **Finding** | FTP Unencrypted Cleartext Login |
| **Severity** | **Medium** | **Port** | TCP: 21 |
| **Target** | 172.28.130.128(21) | | |
| **CVS 3.0**  **Score** | 4.8 | | |
| **Detail** | None | | |
| **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.** | 51 | **Finding** | QuickPHP index.php Remote Source Code Disclosure Vulnerability |
| **Severity** | **Medium** | **Port** | TCP: 2020 |
| **Target** | 172.28.130.128(2020) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **Detail** | None | | |
| **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.** | 52 | **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) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **Detail** | None | | |
| **Solution** | Update to version 7.3.28, 7.4.18 or later. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 53 | **Finding** | SSL/TLS: Report Weak Cipher Suites |
| **Severity** | **Medium** | **Port** | TCP: 443, 3031, 3389 |
| **Target** | 172.28.130.128(3389), 172.28.131.24(3031), 172.28.131.105(3389), 172.28.131.108(3389), 172.28.135.223(3389), 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) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 54 | **Finding** | Apache Tomcat HTTP Request Smuggling Vulnerability (Jul 2021) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **CVS 3.0**  **Score** | 5.3 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 55 | **Finding** | SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability |
| **Severity** | **Medium** | **Port** | TCP: 3389, 7630, 8091, 8181, 8443, 9090, 10102 |
| **Target** | 172.28.130.190(8443), 172.28.131.24(8091, 9090), 172.28.131.49(8181, 10102), 172.28.131.108(3389), 172.28.135.223(3389), 172.28.136.111(3389), 172.28.137.112(7630), 172.28.190.131(3389), 172.28.190.133(3389), 172.28.190.139(3389) | | |
| **CVS 3.0**  **Score** | 4.0 | | |
| **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.** | 56 | **Finding** | Apache Tomcat Security Manager Bypass Vulnerability - Feb16 (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 6.3 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 57 | **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) | | |
| **CVS 3.0**  **Score** | 6.1 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 58 | **Finding** | SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) |
| **Severity** | **Medium** | **Port** | TCP: 443, 3031, 3978, 5007, 5989, 6101, 6301, 7630, 8091, 8443, 9080, 9090, 10102 |
| **Target** | 172.28.130.190(8443), 172.28.131.23(443, 5989, 9080), 172.28.131.24(3031, 8091, 9090), 172.28.131.49(10102), 172.28.131.102(6101, 6301), 172.28.137.112(7630), 172.28.188.168(3978, 5007) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 59 | **Finding** | Apache Tomcat NIO/NIO2 Connectors Information Disclosure Vulnerability (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **CVS 3.0**  **Score** | 5.9 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 60 | **Finding** | Apache Tomcat Request Object Security Bypass Vulnerability (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 61 | **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) | | |
| **CVS 3.0**  **Score** | 5.9 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 62 | **Finding** | Apache Tomcat ServletSecurity Annotations Security Bypass Vulnerability (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 5.8 | | |
| **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.** | 63 | **Finding** | Apache Tomcat Multiple Security Bypass Vulnerabilities (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **Detail** | The flaws are due to errors in the HTTP Digest Access Authentication  implementation,  - which fails to check 'qop' and 'realm' values and allows to bypass  access restrictions.  - Catalina used as the hard-coded server secret in the  DigestAuthenticator.java bypasses cryptographic protection mechanisms.  - which fails to have the expected countermeasures against replay attacks. | | |
| **Solution** | Upgrade Apache Tomcat to 5.5.34, 6.0.33, 7.0.12 or later. | | |
| **Remark** | CVE: CVE-2011-1184 CVE: CVE-2011-5062 CVE: CVE-2011-5063 CVE: CVE-2011-5064 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 64 | **Finding** | Apache Tomcat HTTP/2 Vulnerability - Oct20 (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **CVS 3.0**  **Score** | 4.3 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 65 | **Finding** | Apache Tomcat Directory Disclosure Vulnerability - Feb16 (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 5.3 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 66 | **Finding** | Apache Tomcat Session Fixation Vulnerability (Nov 2012) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 6.8 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 67 | **Finding** | SSL/TLS: Certificate Expired |
| **Severity** | **Medium** | **Port** | TCP: 3031, 7630, 8444 |
| **Target** | 172.28.130.190(8444), 172.28.131.24(3031), 172.28.137.112(7630) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **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.** | 68 | **Finding** | Apache Tomcat Denial Of Service Vulnerability (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 69 | **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) | | |
| **CVS 3.0**  **Score** | 6.5 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 70 | **Finding** | Apache Tomcat Limited Directory Traversal Vulnerability - Feb16 (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 4.3 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 71 | **Finding** | Apache Tomcat SecurityManager Security Bypass Vulnerability - Jun15 (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 72 | **Finding** | Apache Tomcat DoS Vulnerability (Mar 2015) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 6.4 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 73 | **Finding** | Apache Tomcat Multiple Security Bypass Vulnerabilities (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 74 | **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) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 75 | **Finding** | SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits |
| **Severity** | **Medium** | **Port** | TCP: 443, 3031, 8443, 9090 |
| **Target** | 172.28.130.190(8443), 172.28.131.24(443, 3031, 9090) | | |
| **CVS 3.0**  **Score** | 5.3 | | |
| **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.** | 76 | **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) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 77 | **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) | | |
| **CVS 3.0**  **Score** | 5.3 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 78 | **Finding** | Apache Tomcat Hash Collision Denial Of Service Vulnerability |
| **Severity** | **Medium** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 79 | **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) | | |
| **CVS 3.0**  **Score** | 5.9 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 80 | **Finding** | SSL/TLS: Certificate Signed Using A Weak Signature Algorithm |
| **Severity** | **Medium** | **Port** | TCP: 3031, 8443 |
| **Target** | 172.28.130.190(8443), 172.28.131.24(3031) | | |
| **CVS 3.0**  **Score** | 4.0 | | |
| **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.** | 81 | **Finding** | Apache Tomcat Open Redirect Vulnerability (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 8081, 8444 |
| **Target** | 172.28.130.190(8081, 8444) | | |
| **CVS 3.0**  **Score** | 4.3 | | |
| **Detail** | None | | |
| **Solution** | Update to version 7.0.91, 8.5.34, 9.0.12 or later. | | |
| **Remark** | CVE: CVE-2018-11784 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 82 | **Finding** | Weak Encryption Algorithm(s) Supported (SSH) |
| **Severity** | **Medium** | **Port** | TCP: 22 |
| **Target** | 172.28.131.23(22), 172.28.131.24(22), 172.28.188.167(22), 172.28.188.168(22) | | |
| **CVS 3.0**  **Score** | 4.3 | | |
| **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.** | 83 | **Finding** | SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection |
| **Severity** | **Medium** | **Port** | TCP: 3031 |
| **Target** | 172.28.131.24(3031) | | |
| **CVS 3.0**  **Score** | 5.9 | | |
| **Detail** | The SSLv2 and SSLv3 protocols contain known cryptographic  flaws like:  - CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)  - CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN) | | |
| **Solution** | It is recommended to disable the deprecated SSLv2 and/or SSLv3  protocols in favor of the TLSv1.2+ protocols. Please see the references for more information. | | |
| **Remark** | CVE: CVE-2016-0800 CVE: CVE-2014-3566 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 84 | **Finding** | jQuery 1.9.0 XSS Vulnerability |
| **Severity** | **Medium** | **Port** | TCP: 8090, 8091 |
| **Target** | 172.28.131.24(8090, 8091) | | |
| **CVS 3.0**  **Score** | 6.1 | | |
| **Detail** | The jQuery(strInput) function does not differentiate selectors  from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was  HTML by looking for the '' character anywhere in the string, giving attackers more flexibility  when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input  to be HTML if it explicitly starts with the '' character, limiting exploitability only to  attackers who can control the beginning of a string, which is far less common. | | |
| **Solution** | Update to version 1.9.0 or later. | | |
| **Remark** | CVE: CVE-2012-6708 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 85 | **Finding** | SSL/TLS: Report Anonymous Cipher Suites |
| **Severity** | **Medium** | **Port** | TCP: 6101, 6301 |
| **Target** | 172.28.131.102(6101, 6301) | | |
| **CVS 3.0**  **Score** | 5.4 | | |
| **Detail** | Services supporting 'Anonymous' cipher suites could allow a  client to negotiate an SSL/TLS connection to the host without any authentication of the remote  endpoint. | | |
| **Solution** | The configuration of this services should be changed so  that it does not accept the listed 'Anonymous' cipher suites anymore.  Please see the references for more resources supporting you in this task. | | |
| **Remark** | CVE: CVE-2007-1858 CVE: CVE-2014-0351 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 86 | **Finding** | Oracle MySQL Server = 5.7.36 / 8.0 = 8.0.27 Security Update (cpujan2022) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 5.5 | | |
| **Detail** | None | | |
| **Solution** | Update to version 5.7.37, 8.0.28 or later. | | |
| **Remark** | CVE: CVE-2021-22946 CVE: CVE-2022-21367 CVE: CVE-2022-21270 CVE: CVE-2022-21304 CVE: CVE-2022-21344 CVE: CVE-2022-21303 CVE: CVE-2022-21245 CVE: CVE-2021-22947 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 87 | **Finding** | Oracle MySQL Server = 5.6.50 / 5.7 = 5.7.32 / 8.0 = 8.0.22 Security Update (cpujan2021) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 4.9 | | |
| **Detail** | None | | |
| **Solution** | Update to version 5.6.51, 5.7.33, 8.0.23 or later. | | |
| **Remark** | CVE: CVE-2021-2022 CVE: CVE-2021-2060 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 88 | **Finding** | Oracle Mysql Security Updates (oct2017-3236626) 04 - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 6.5 | | |
| **Detail** | Multiple flaws exist due to:  - An error in 'Client programs' component.  - An error in 'Server: DDL'.  - An error in 'Server: Replication' | | |
| **Solution** | Apply the patch from the referenced advisory. | | |
| **Remark** | CVE: CVE-2017-10379 CVE: CVE-2017-10384 CVE: CVE-2017-10268 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 89 | **Finding** | Oracle MySQL Server = 5.7.30 / 8.0 = 8.0.17 Security Update (cpuapr2021) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 4.9 | | |
| **Detail** | None | | |
| **Solution** | Update to version 5.7.31, 8.0.18 or later. | | |
| **Remark** | CVE: CVE-2021-2160 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 90 | **Finding** | Oracle Mysql Security Updates (jul2017-3236622) 02 - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 4.2 | | |
| **Detail** | Multiple flaws exist due to   - A flaw in the Client mysqldump component.   - A flaw in the Server: DDL component.   - A flaw in the C API component.   - A flaw in the Connector/C component.   - A flaw in the Server: Charsets component. | | |
| **Solution** | Apply the patch from the referenced advisory. | | |
| **Remark** | CVE: CVE-2017-3651 CVE: CVE-2017-3653 CVE: CVE-2017-3652 CVE: CVE-2017-3635 CVE: CVE-2017-3648 CVE: CVE-2017-3641 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 91 | **Finding** | Oracle Mysql Security Updates (jul2017-3236622) 03 - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 5.3 | | |
| **Detail** | The flaw exists due to an error in the Client  programs component. | | |
| **Solution** | Apply the patch from the referenced advisory. | | |
| **Remark** | CVE: CVE-2017-3636 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 92 | **Finding** | Oracle MySQL Server = 5.6.42 / 5.7 = 5.7.24 / 8.0 = 8.0.13 Security Update (cpuapr2019) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 5.9 | | |
| **Detail** | Difficult to exploit vulnerability allows unauthenticated attacker with  network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can  result in unauthorized access to critical data or complete access to all MySQL Server accessible data. | | |
| **Solution** | Update to version 5.6.43, 5.7.25, 8.0.14 or later. | | |
| **Remark** | CVE: CVE-2018-3123 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 93 | **Finding** | Oracle Mysql Security Updates (jan2018-3236628) 02 - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 6.5 | | |
| **Detail** | Multiple flaws exist due to:  - An error in the 'Server: DDL' component.  - Multiple errors in the 'Server: Optimizer' component. | | |
| **Solution** | Apply the patch from the referenced advisory. | | |
| **Remark** | CVE: CVE-2018-2668 CVE: CVE-2018-2665 CVE: CVE-2018-2622 CVE: CVE-2018-2640 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 94 | **Finding** | Oracle MySQL Server = 5.6.45 / 5.7 = 5.7.27 Security Update (cpuoct2019) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 5.3 | | |
| **Detail** | Oracle MySQL Server is prone to multiple vulnerabilities.  For further information refer to the official advisory via the referenced link. | | |
| **Solution** | Update to version 5.6.46, 5.7.28 or later. | | |
| **Remark** | CVE: CVE-2019-2922 CVE: CVE-2019-2923 CVE: CVE-2019-2924 CVE: CVE-2019-2910 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 95 | **Finding** | Oracle MySQL Server = 5.7.32 / 8.0 = 8.0.22 Security Update (cpuapr2021) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 5.9 | | |
| **Detail** | None | | |
| **Solution** | Update to version 5.7.33, 8.0.23 or later. | | |
| **Remark** | CVE: CVE-2020-1971 CVE: CVE-2021-2178 CVE: CVE-2021-2202 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 96 | **Finding** | Oracle MySQL Server = 5.7.34 / 8.0 = 8.0.25 Security Update (cpujul2021) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 5.9 | | |
| **Detail** | None | | |
| **Solution** | Update to version 5.7.35, 8.0.26 or later. | | |
| **Remark** | CVE: CVE-2021-22901 CVE: CVE-2019-17543 CVE: CVE-2021-2389 CVE: CVE-2021-2390 CVE: CVE-2021-2356 CVE: CVE-2021-2385 CVE: CVE-2021-2342 CVE: CVE-2021-2372 CVE: CVE-2021-22897 CVE: CVE-2021-22898 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 97 | **Finding** | Oracle Mysql Security Updates (apr2018-3678067) 04 - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 5.9 | | |
| **Detail** | Multiple flaws exist due to  - Multiple errors in the 'Client programs' component of MySQL Server.  - An error in the 'Server: Locking' component of MySQL Server.  - An error in the 'Server: Optimizer' component of MySQL Server.  - Multiple errors in the 'Server: DDL' component of MySQL Server.  - Multiple errors in the 'Server: Replication' component of MySQL Server.  - An error in the 'InnoDB' component of MySQL Server.  - An error in the 'Server : Security : Privileges' component of MySQL Server. | | |
| **Solution** | Apply the latest patch from vendor. Please see the references for more information. | | |
| **Remark** | CVE: CVE-2018-2761 CVE: CVE-2018-2771 CVE: CVE-2018-2781 CVE: CVE-2018-2773 CVE: CVE-2018-2817 CVE: CVE-2018-2813 CVE: CVE-2018-2755 CVE: CVE-2018-2819 CVE: CVE-2018-2818 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 98 | **Finding** | Oracle MySQL Server = 5.6.44 / 5.7 = 5.7.26 / 8.0 = 8.0.16 Security Update (cpuoct2019) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 6.2 | | |
| **Detail** | Easily exploitable vulnerability allows unauthenticated attacker with logon to  the infrastructure where MySQL Server executes to compromise MySQL Server. | | |
| **Solution** | Update to version 5.6.45, 5.7.27, 8.0.17 or later. | | |
| **Remark** | CVE: CVE-2019-2969 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 99 | **Finding** | Oracle MySQL Server = 5.6.49 / 5.7 = 5.7.31 / 8.0 = 8.0.21 Security Update (cpuoct2020) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 6.5 | | |
| **Detail** | None | | |
| **Solution** | Update to version 5.6.50, 5.7.32, 8.0.22 or later. | | |
| **Remark** | CVE: CVE-2020-14765 CVE: CVE-2020-14769 CVE: CVE-2020-14812 CVE: CVE-2020-14793 CVE: CVE-2020-14672 CVE: CVE-2020-14867 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 100 | **Finding** | Oracle MySQL Security Update (cpujul2018 - 04) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 4.9 | | |
| **Detail** | Multiple flaws exist due to an error in the  'Server: Security: Privileges' component of MySQL Server. | | |
| **Solution** | The vendor has released updates. Please see the references for  more information. | | |
| **Remark** | CVE: CVE-2018-3063 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 101 | **Finding** | Oracle MySQL Server = 5.6.46 / 5.7 = 5.7.26 Security Update (cpuapr2020) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 5.3 | | |
| **Detail** | None | | |
| **Solution** | Update to version 5.6.47, 5.7.27 or later. | | |
| **Remark** | CVE: CVE-2019-1547 CVE: CVE-2019-1549 CVE: CVE-2019-1552 CVE: CVE-2019-1563 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 102 | **Finding** | Oracle MySQL Server = 5.6.44 / 5.7 = 5.7.26 / 8.0 = 8.0.16 Security Update (cpujul2019) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 5.5 | | |
| **Detail** | Oracle MySQL Server is prone to multiple denial of service vulnerabilities.  For further information refer to the official advisory via the referenced link. | | |
| **Solution** | Update to version 5.6.45, 5.7.27, 8.0.17 or later. | | |
| **Remark** | CVE: CVE-2019-2805 CVE: CVE-2019-2740 CVE: CVE-2019-2819 CVE: CVE-2019-2739 CVE: CVE-2019-2737 CVE: CVE-2019-2738 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 103 | **Finding** | Oracle MySQL Server = 5.6.46 Security Update (cpujan2020) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 6.5 | | |
| **Detail** | None | | |
| **Solution** | Update to version 5.6.47 or later. | | |
| **Remark** | CVE: CVE-2020-2579 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 104 | **Finding** | Oracle MySQL Backronym Vulnerability June16 (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 5.9 | | |
| **Detail** | The flaw exists due to improper validation  of MySQL client library when establishing a secure connection to a MySQL  server using the --ssl option. | | |
| **Solution** | Upgrade to version Oracle MySQL Server 5.7.3 or  later. | | |
| **Remark** | CVE: CVE-2015-3152 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 105 | **Finding** | Oracle MySQL Server = 5.7.33 Security Update (cpuapr2021) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 4.9 | | |
| **Detail** | None | | |
| **Solution** | Update to version 5.7.34 or later. | | |
| **Remark** | CVE: CVE-2021-2154 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 106 | **Finding** | Oracle Mysql Security Updates (oct2017-3236626) 02 - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 6.5 | | |
| **Detail** | The flaw exists due to an error in  'Server: Optimizer' | | |
| **Solution** | Apply the patch from the referenced advisory. | | |
| **Remark** | CVE: CVE-2017-10378 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 107 | **Finding** | Oracle MySQL Server = 5.6.45 / 5.7 = 5.7.27 / 8.0 = 8.0.17 Security Update (cpuoct2019) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 6.5 | | |
| **Detail** | Oracle MySQL Server is prone to multiple vulnerabilities.  For further information refer to the official advisory via the referenced link. | | |
| **Solution** | Update to version 5.6.46, 5.7.28, 8.0.18 or later. | | |
| **Remark** | CVE: CVE-2019-2974 CVE: CVE-2019-2911 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 108 | **Finding** | Oracle MySQL Server = 5.6.50 / 5.7 = 5.7.30 / 8.0 = 8.0.17 Security Update (cpujan2021) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 4.9 | | |
| **Detail** | None | | |
| **Solution** | Update to version 5.6.51, 5.7.31, 8.0.18 or later. | | |
| **Remark** | CVE: CVE-2021-2001 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 109 | **Finding** | Oracle MySQL Server = 5.6.43 / 5.7 = 5.7.25 / 8.0 = 8.0.15 Security Update (cpuapr2019) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 5.9 | | |
| **Detail** | The attacks range in variety and difficulty. Most of them allow an attacker  with network access via multiple protocols to compromise the MySQL Server.  For further information refer to the official advisory via the referenced link. | | |
| **Solution** | Update to version 5.6.44, 5.7.26, 8.0.16 or later. | | |
| **Remark** | CVE: CVE-2019-1559 CVE: CVE-2019-2683 CVE: CVE-2019-2627 CVE: CVE-2019-2614 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 110 | **Finding** | VNC Server Unencrypted Data Transmission |
| **Severity** | **Medium** | **Port** | TCP: 5900 |
| **Target** | 172.28.135.223(5900) | | |
| **CVS 3.0**  **Score** | 4.8 | | |
| **Detail** | None | | |
| **Solution** | Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254].  Some VNC server vendors are also providing more secure Security Types within their products. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 111 | **Finding** | Weak Host Key Algorithm(s) (SSH) |
| **Severity** | **Medium** | **Port** | TCP: 22 |
| **Target** | 172.28.137.52(22), 172.28.137.112(22) | | |
| **CVS 3.0**  **Score** | 5.3 | | |
| **Detail** | None | | |
| **Solution** | Disable the reported weak host key algorithm(s). | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 112 | **Finding** | OpenSSH sftp-server Security Bypass Vulnerability (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 22 |
| **Target** | 172.28.137.112(22) | | |
| **CVS 3.0**  **Score** | 5.3 | | |
| **Detail** | The flaw exists in the 'process\_open' function  in sftp-server.c script which does not properly prevent write operations in  readonly mode. | | |
| **Solution** | Upgrade to OpenSSH version 7.6 or later. | | |
| **Remark** | CVE: CVE-2017-15906 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 113 | **Finding** | OpenSSH auth2-gss.c User Enumeration Vulnerability - Windows |
| **Severity** | **Medium** | **Port** | TCP: 22 |
| **Target** | 172.28.137.112(22) | | |
| **CVS 3.0**  **Score** | 5.3 | | |
| **Detail** | The flaw exists in the 'auth-gss2.c' source code file of the  affected software and is due to insufficient validation of an authentication request packet when  the Guide Star Server II (GSS2) component is used on an affected system. | | |
| **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** | CVE: CVE-2018-15919 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 114 | **Finding** | OpenSSH 7.8 User Enumeration Vulnerability - Windows |
| **Severity** | **Medium** | **Port** | TCP: 22 |
| **Target** | 172.28.137.112(22) | | |
| **CVS 3.0**  **Score** | 5.3 | | |
| **Detail** | The flaw is due to not delaying bailout for an invalid  authenticating user until after the packet containing the request has been fully parsed, related  to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c | | |
| **Solution** | Update to version 7.8 or later. | | |
| **Remark** | CVE: CVE-2018-15473 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 115 | **Finding** | SSL/TLS: Missing `secure` Cookie Attribute |
| **Severity** | **Medium** | **Port** | TCP: 7630 |
| **Target** | 172.28.137.112(7630) | | |
| **CVS 3.0**  **Score** | 6.4 | | |
| **Detail** | The flaw is due to cookie is not using 'secure' attribute, which  allows cookie to be passed to the server by the client over non-secure channels (http) and allows attacker  to conduct session hijacking attacks. | | |
| **Solution** | Set the 'secure' attribute for any cookies that are sent over a SSL/TLS connection. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 116 | **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) | | |
| **CVS 3.0**  **Score** | 5.3 | | |
| **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.** | 117 | **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) | | |
| **CVS 3.0**  **Score** | 5.0 | | |
| **Detail** | None | | |
| **Solution** | Replace the SSL/TLS certificate with one signed by a trusted  CA. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 118 | **Finding** | TCP timestamps |
| **Severity** | **Low** | **Port** | TCP: 0 |
| **Target** | 172.28.130.128(0), 172.28.130.190(0), 172.28.131.23(0), 172.28.131.24(0), 172.28.131.48(0), 172.28.131.102(0), 172.28.131.105(0), 172.28.131.108(0), 172.28.135.188(0), 172.28.135.189(0), 172.28.135.223(0), 172.28.136.111(0), 172.28.136.118(0), 172.28.136.153(0), 172.28.137.112(0), 172.28.188.167(0), 172.28.188.168(0), 172.28.190.131(0), 172.28.190.133(0), 172.28.190.139(0) | | |
| **CVS 3.0**  **Score** | 2.6 | | |
| **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.** | 119 | **Finding** | Apache Tomcat Information Disclosure Vulnerability (May 2013) - Windows |
| **Severity** | **Low** | **Port** | TCP: 443, 8080, 8443 |
| **Target** | 172.28.130.190(443, 8080, 8443) | | |
| **CVS 3.0**  **Score** | 2.6 | | |
| **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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 120 | **Finding** | SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) |
| **Severity** | **Low** | **Port** | TCP: 3031 |
| **Target** | 172.28.131.24(3031) | | |
| **CVS 3.0**  **Score** | 3.4 | | |
| **Detail** | The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code | | |
| **Solution** | Possible Mitigations are:   - Disable SSLv3   - Disable cipher suites supporting CBC cipher modes   - Enable TLS\_FALLBACK\_SCSV if the service is providing TLSv1.0+ | | |
| **Remark** | CVE: CVE-2014-3566 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 121 | **Finding** | Oracle MySQL Security Update (cpujul2018 - 02) - Windows |
| **Severity** | **Low** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 3.3 | | |
| **Detail** | Multiple flaws exist due to errors in  'Server: Security: Encryption', 'Server: Options', 'MyISAM', 'Client mysqldump'  components of application. | | |
| **Solution** | The vendor has released updates. Please see the references for  more information. | | |
| **Remark** | CVE: CVE-2018-2767 CVE: CVE-2018-3066 CVE: CVE-2018-3058 CVE: CVE-2018-3070 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 122 | **Finding** | Oracle MySQL Server = 5.6.44 / 5.7 = 5.7.18 Security Update (cpujul2019) - Windows |
| **Severity** | **Low** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **CVS 3.0**  **Score** | 2.7 | | |
| **Detail** | None | | |
| **Solution** | Update to version 5.6.45, 5.7.19 or later. | | |
| **Remark** | CVE: CVE-2019-2730 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 123 | **Finding** | Weak MAC Algorithm(s) Supported (SSH) |
| **Severity** | **Low** | **Port** | TCP: 22 |
| **Target** | 172.28.188.167(22), 172.28.188.168(22) | | |
| **CVS 3.0**  **Score** | 2.6 | | |
| **Detail** | None | | |
| **Solution** | Disable the reported weak MAC algorithm(s). | | |
| **Remark** |  | | |



# 6 Port Discovery

| **Port** | **Protocol** | **Service** |
| --- | --- | --- |
| 22 | tcp | ssh |
| 80 | tcp | http |
| 81 | tcp | hosts2-ns |
| 111 | tcp | rpcbind |
| 135 | tcp | msrpc |
| 139 | tcp | netbios-ssn |
| 427 | tcp | svrloc |
| 443 | tcp | https |
| 445 | tcp | microsoft-ds |
| 902 | tcp | iss-realsecure |
| 1007 | tcp | unknown |
| 1010 | tcp | surf |
| 1011 | tcp | unknown |
| 1433 | tcp | ms-sql-s |
| 1556 | tcp | veritas\_pbx |
| 2007 | tcp | dectalk |
| 3011 | tcp | trusted-web |
| 3031 | tcp | eppc |
| 3211 | tcp | avsecuremgmt |
| 3301 | tcp | unknown |
| 3306 | tcp | mysql |
| 3389 | tcp | ms-wbt-server |
| 4000 | tcp | remoteanything |
| 4045 | tcp | lockd |
| 4848 | tcp | appserv-http |
| 5432 | tcp | postgresql |
| 5800 | tcp | vnc-http |
| 5900 | tcp | vnc |
| 5989 | tcp | wbem-https |
| 6001 | tcp | X11:1 |
| 6101 | tcp | backupexec |
| 7000 | tcp | afs3-fileserver |
| 8000 | tcp | http-alt |
| 8001 | tcp | vcom-tunnel |
| 8080 | tcp | http-proxy |
| 8081 | tcp | blackice-icecap |
| 8090 | tcp | opsmessaging |
| 8181 | tcp | intermapper |
| 8300 | tcp | tmi |
| 9000 | tcp | cslistener |
| 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 |