**Vulnerability Assessment Report**

**For**



**SIPH phase 2 greenbone**

**April 07, 2022**

**Document Security Level:** Confidential

**Document Version:** 1.0

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

|  |  |  |  |
| --- | --- | --- | --- |
| SIPH phase 2 greenbone | | INET Managed Services CO., LTD. | |
| Name |  | **Name** |  |
| Position |  | **Position** |  |
| Tel |  | **Tel** |  |
| Signature |  | **Signature** |  |

**Table of Contents**

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

[2. Operation Method 5](#_Toc98507703)

[3. Project Scope 6](#_Toc98507704)

[3.1 Infrastructure Vulnerability Assessment 6](#_Toc98507705)

[4. Testing Tools 7](#_Toc98507706)

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

[5.1 Target Information 8](#_Toc98507708)

[5.2 Executive summary 9](#_Toc98507709)

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

[5.2.2 Vulnerability by Target 9](#_Toc98507711)

[5.3 Infrastructure Vulnerability Detail 10](#_Toc98507712)

[6. Appendix 11](#_Toc98507713)

[6.1 About Nessus 11](#_Toc98507714)

[6.1.1 Nessus vulnerabilities 11](#_Toc98507715)

[6.1.2 Nessus risk score 11](#_Toc98507716)

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

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

# Restrictions on disclosure and use of information

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

# Operation Method

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



Figure 1: Operation Method

# Project Scope

## **3.1 Infrastructure Vulnerability Assessment**

**Target / IP Address:**

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

# Testing Tools

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

# Infrastructure Vulnerability Assessment

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

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

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

Diagram

Description automatically generated

Figure 2: Vulnerability Assessment from Public Access

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

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

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

A picture containing diagram

Description automatically generated

Figure 3: Vulnerability Assessment from Private Access

## **5.1 Target Information**

| **No.** | **Domain / Server Name** | **IP Address** | **OS/Model** | **Port** |
| --- | --- | --- | --- | --- |
| 1 | - | test | - | test |

## **5.2 Executive summary**

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

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

A picture containing text, gambling house

Description automatically generated

Figure 4: Summary by Severity of Infrastructure Vulnerability Assessment

### **5.2.2 Vulnerability by Target**

| **No.** | **Domain/Server Name** | **IP Address** | **Critical** | **High** | **Medium** | **Low** | **Total** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | - | 172.28.131.23 | 0 | 0 | 7 | 1 | 8 |
| 2 | - | 172.28.131.24 | 0 | 1 | 17 | 2 | 20 |
| 3 | - | 172.28.131.48 | 0 | 0 | 2 | 1 | 3 |
| 4 | - | 172.28.131.49 | 0 | 1 | 7 | 0 | 8 |
| 5 | - | 172.28.131.102 | 0 | 0 | 9 | 1 | 10 |
| 6 | - | 172.28.131.105 | 0 | 0 | 4 | 1 | 5 |
| 7 | - | 172.28.131.108 | 0 | 8 | 28 | 3 | 39 |
| 8 | - | 172.28.135.223 | 0 | 0 | 5 | 1 | 6 |
| 9 | - | 172.28.136.118 | 0 | 0 | 3 | 1 | 4 |
| 10 | - | 172.28.136.153 | 0 | 1 | 4 | 1 | 6 |
| 11 | - | 172.28.137.52 | 0 | 0 | 6 | 0 | 6 |
| 12 | - | 172.28.190.131 | 0 | 0 | 4 | 1 | 5 |
| 13 | - | 172.28.190.133 | 0 | 0 | 6 | 1 | 7 |
| **Total** | | | 0 | 11 | 102 | 14 | 127 |

## **5.3 Infrastructure Vulnerability Detail**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 1 | **Finding** | SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability |
| **Severity** | **High** | **Port** | TCP: 3031 |
| **Target** | 172.28.131.24(3031) | | |
| **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 CERT: DFN-CERT-2016-0388 CERT: DFN-CERT-2015-0593 CERT: DFN-CERT-2015-0427 CERT: DFN-CERT-2015-0396 CERT: DFN-CERT-2015-0082 CERT: DFN-CERT-2015-0079 CERT: DFN-CERT-2015-0078 CERT: DFN-CERT-2014-1717 CERT: DFN-CERT-2014-1632 CERT: DFN-CERT-2014-1364 CERT: DFN-CERT-2014-1357 CERT: DFN-CERT-2014-1350 CERT: DFN-CERT-2014-1265 CERT: DFN-CERT-2014-1209 CERT: DFN-CERT-2014-0917 CERT: DFN-CERT-2014-0789 CERT: DFN-CERT-2014-0778 CERT: DFN-CERT-2014-0768 CERT: DFN-CERT-2014-0752 CERT: DFN-CERT-2014-0747 CERT: DFN-CERT-2014-0738 CERT: DFN-CERT-2014-0715 CERT: DFN-CERT-2014-0714 CERT: DFN-CERT-2014-0709 CERT: CB-K15/0567 CERT: CB-K15/0415 CERT: CB-K15/0384 CERT: CB-K15/0080 CERT: CB-K15/0079 CERT: CB-K15/0074 CERT: CB-K14/1617 CERT: CB-K14/1537 CERT: CB-K14/1299 CERT: CB-K14/1297 CERT: CB-K14/1294 CERT: CB-K14/1202 CERT: CB-K14/1174 CERT: CB-K14/1153 CERT: CB-K14/0876 CERT: CB-K14/0756 CERT: CB-K14/0746 CERT: CB-K14/0736 CERT: CB-K14/0722 CERT: CB-K14/0716 CERT: CB-K14/0708 CERT: CB-K14/0684 CERT: CB-K14/0683 CERT: CB-K14/0680 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 2 | **Finding** | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS |
| **Severity** | **High** | **Port** | TCP: 443, 10102 |
| **Target** | 172.28.131.49(10102), 172.28.136.153(443) | | |
| **Detail** | These rules are applied for the evaluation of the vulnerable cipher suites:   - 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183). | | |
| **Solution** | The configuration of this services should be changed so  that it does not accept the listed cipher suites anymore.   Please see the references for more resources supporting you with this task. | | |
| **Remark** | CVE: CVE-2016-2183 CVE: CVE-2016-6329 CVE: CVE-2020-12872 CERT: DFN-CERT-2021-1618 CERT: DFN-CERT-2021-0775 CERT: DFN-CERT-2021-0770 CERT: DFN-CERT-2021-0274 CERT: DFN-CERT-2020-2141 CERT: DFN-CERT-2020-0368 CERT: DFN-CERT-2019-1455 CERT: DFN-CERT-2019-0068 CERT: DFN-CERT-2018-1296 CERT: DFN-CERT-2018-0323 CERT: DFN-CERT-2017-2070 CERT: DFN-CERT-2017-1954 CERT: DFN-CERT-2017-1885 CERT: DFN-CERT-2017-1831 CERT: DFN-CERT-2017-1821 CERT: DFN-CERT-2017-1785 CERT: DFN-CERT-2017-1626 CERT: DFN-CERT-2017-1326 CERT: DFN-CERT-2017-1239 CERT: DFN-CERT-2017-1238 CERT: DFN-CERT-2017-1090 CERT: DFN-CERT-2017-1060 CERT: DFN-CERT-2017-0968 CERT: DFN-CERT-2017-0947 CERT: DFN-CERT-2017-0946 CERT: DFN-CERT-2017-0904 CERT: DFN-CERT-2017-0816 CERT: DFN-CERT-2017-0746 CERT: DFN-CERT-2017-0677 CERT: DFN-CERT-2017-0675 CERT: DFN-CERT-2017-0611 CERT: DFN-CERT-2017-0609 CERT: DFN-CERT-2017-0522 CERT: DFN-CERT-2017-0519 CERT: DFN-CERT-2017-0482 CERT: DFN-CERT-2017-0351 CERT: DFN-CERT-2017-0090 CERT: DFN-CERT-2017-0089 CERT: DFN-CERT-2017-0088 CERT: DFN-CERT-2017-0086 CERT: DFN-CERT-2016-1943 CERT: DFN-CERT-2016-1937 CERT: DFN-CERT-2016-1732 CERT: DFN-CERT-2016-1726 CERT: DFN-CERT-2016-1715 CERT: DFN-CERT-2016-1714 CERT: DFN-CERT-2016-1588 CERT: DFN-CERT-2016-1555 CERT: DFN-CERT-2016-1391 CERT: DFN-CERT-2016-1378 CERT: CB-K21/1094 CERT: CB-K20/1023 CERT: CB-K20/0321 CERT: CB-K20/0314 CERT: CB-K20/0157 CERT: CB-K19/0618 CERT: CB-K19/0615 CERT: CB-K18/0296 CERT: CB-K17/1980 CERT: CB-K17/1871 CERT: CB-K17/1803 CERT: CB-K17/1753 CERT: CB-K17/1750 CERT: CB-K17/1709 CERT: CB-K17/1558 CERT: CB-K17/1273 CERT: CB-K17/1202 CERT: CB-K17/1196 CERT: CB-K17/1055 CERT: CB-K17/1026 CERT: CB-K17/0939 CERT: CB-K17/0917 CERT: CB-K17/0915 CERT: CB-K17/0877 CERT: CB-K17/0796 CERT: CB-K17/0724 CERT: CB-K17/0661 CERT: CB-K17/0657 CERT: CB-K17/0582 CERT: CB-K17/0581 CERT: CB-K17/0506 CERT: CB-K17/0504 CERT: CB-K17/0467 CERT: CB-K17/0345 CERT: CB-K17/0098 CERT: CB-K17/0089 CERT: CB-K17/0086 CERT: CB-K17/0082 CERT: CB-K16/1837 CERT: CB-K16/1830 CERT: CB-K16/1635 CERT: CB-K16/1630 CERT: CB-K16/1624 CERT: CB-K16/1622 CERT: CB-K16/1500 CERT: CB-K16/1465 CERT: CB-K16/1307 CERT: CB-K16/1296 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 3 | **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) | | |
| **Detail** |  | | |
| **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 CERT: DFN-CERT-2022-0586 CERT: DFN-CERT-2022-0437 CERT: DFN-CERT-2022-0369 CERT: DFN-CERT-2022-0122 CERT: DFN-CERT-2022-0120 CERT: DFN-CERT-2022-0118 CERT: DFN-CERT-2022-0112 CERT: DFN-CERT-2022-0076 CERT: DFN-CERT-2022-0052 CERT: DFN-CERT-2022-0031 CERT: DFN-CERT-2021-2527 CERT: DFN-CERT-2021-2502 CERT: DFN-CERT-2021-2481 CERT: DFN-CERT-2021-2438 CERT: DFN-CERT-2021-2434 CERT: DFN-CERT-2021-2403 CERT: DFN-CERT-2021-2394 CERT: DFN-CERT-2021-2369 CERT: DFN-CERT-2021-2329 CERT: DFN-CERT-2021-2223 CERT: DFN-CERT-2021-2216 CERT: DFN-CERT-2021-2214 CERT: DFN-CERT-2021-2189 CERT: DFN-CERT-2021-2188 CERT: DFN-CERT-2021-2185 CERT: DFN-CERT-2021-2167 CERT: DFN-CERT-2021-1996 CERT: DFN-CERT-2021-1931 CERT: DFN-CERT-2021-1917 CERT: DFN-CERT-2021-1915 CERT: DFN-CERT-2021-1871 CERT: DFN-CERT-2021-1803 CERT: DFN-CERT-2021-1799 CERT: DFN-CERT-2021-1743 CERT: DFN-CERT-2021-1593 CERT: DFN-CERT-2021-1580 CERT: DFN-CERT-2021-1568 CERT: CB-K22/0316 CERT: CB-K22/0224 CERT: CB-K22/0077 CERT: CB-K22/0072 CERT: CB-K22/0062 CERT: CB-K22/0045 CERT: CB-K22/0030 CERT: CB-K22/0011 CERT: CB-K21/1268 CERT: CB-K21/1179 CERT: CB-K21/1161 CERT: CB-K21/1087 CERT: CB-K21/0994 CERT: CB-K21/0991 CERT: CB-K21/0969 CERT: CB-K21/0907 CERT: CB-K21/0897 CERT: CB-K21/0797 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 4 | **Finding** | Oracle Mysql Security Update (cpuoct2018 - 02) - Windows |
| **Severity** | **High** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **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 CERT: DFN-CERT-2020-1536 CERT: DFN-CERT-2019-1614 CERT: DFN-CERT-2019-1588 CERT: DFN-CERT-2019-1152 CERT: DFN-CERT-2019-1047 CERT: DFN-CERT-2019-0592 CERT: DFN-CERT-2019-0484 CERT: DFN-CERT-2019-0463 CERT: DFN-CERT-2019-0112 CERT: DFN-CERT-2018-2435 CERT: DFN-CERT-2018-2273 CERT: DFN-CERT-2018-2110 CERT: DFN-CERT-2018-1408 CERT: DFN-CERT-2018-0659 CERT: DFN-CERT-2018-0645 CERT: DFN-CERT-2018-0039 CERT: DFN-CERT-2017-2300 CERT: DFN-CERT-2017-2268 CERT: DFN-CERT-2017-1825 CERT: DFN-CERT-2017-1785 CERT: DFN-CERT-2017-1692 CERT: DFN-CERT-2017-1655 CERT: DFN-CERT-2017-1097 CERT: DFN-CERT-2017-0904 CERT: DFN-CERT-2017-0806 CERT: DFN-CERT-2016-2109 CERT: CB-K22/0045 CERT: CB-K20/0714 CERT: CB-K18/1005 CERT: CB-K18/0799 CERT: CB-K18/0030 CERT: CB-K17/2199 CERT: CB-K17/2168 CERT: CB-K17/1745 CERT: CB-K17/1709 CERT: CB-K17/1622 CERT: CB-K17/1585 CERT: CB-K17/1062 CERT: CB-K17/0877 CERT: CB-K17/0784 CERT: CB-K16/1996 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 5 | **Finding** | Oracle MySQL Denial Of Service Vulnerability Feb17 (Windows) |
| **Severity** | **High** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **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 CERT: DFN-CERT-2018-1276 CERT: DFN-CERT-2018-0242 CERT: DFN-CERT-2017-1675 CERT: DFN-CERT-2017-1341 CERT: DFN-CERT-2017-1282 CERT: DFN-CERT-2017-0675 CERT: DFN-CERT-2017-0430 CERT: CB-K18/0224 CERT: CB-K17/1604 CERT: CB-K17/1298 CERT: CB-K17/1239 CERT: CB-K17/0657 CERT: CB-K17/0423 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 6 | **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) | | |
| **Detail** |  | | |
| **Solution** | Update to version 5.7.30, 8.0.20 or later. | | |
| **Remark** | CVE: CVE-2021-2144 CERT: DFN-CERT-2021-0821 CERT: CB-K21/0421 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 7 | **Finding** | Oracle Mysql Security Updates (jan2018-3236628) 04 - Windows |
| **Severity** | **High** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **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 CERT: DFN-CERT-2019-1047 CERT: DFN-CERT-2018-1276 CERT: DFN-CERT-2018-1265 CERT: DFN-CERT-2018-0733 CERT: DFN-CERT-2018-0515 CERT: DFN-CERT-2018-0424 CERT: DFN-CERT-2018-0286 CERT: DFN-CERT-2018-0101 CERT: CB-K18/0480 CERT: CB-K18/0392 CERT: CB-K18/0265 CERT: CB-K18/0096 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 8 | **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) | | |
| **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 CERT: DFN-CERT-2020-0326 CERT: DFN-CERT-2019-2457 CERT: DFN-CERT-2019-2456 CERT: DFN-CERT-2019-2305 CERT: DFN-CERT-2019-2300 CERT: DFN-CERT-2019-2046 CERT: DFN-CERT-2019-1996 CERT: DFN-CERT-2019-1897 CERT: DFN-CERT-2019-1746 CERT: DFN-CERT-2019-1713 CERT: DFN-CERT-2019-1617 CERT: DFN-CERT-2019-1614 CERT: DFN-CERT-2019-1600 CERT: DFN-CERT-2019-1588 CERT: DFN-CERT-2019-1562 CERT: DFN-CERT-2019-1455 CERT: DFN-CERT-2019-1450 CERT: DFN-CERT-2019-1240 CERT: DFN-CERT-2019-1152 CERT: DFN-CERT-2019-1047 CERT: DFN-CERT-2019-0782 CERT: DFN-CERT-2019-0781 CERT: DFN-CERT-2019-0778 CERT: DFN-CERT-2019-0775 CERT: DFN-CERT-2019-0772 CERT: DFN-CERT-2019-0484 CERT: DFN-CERT-2019-0232 CERT: DFN-CERT-2019-0204 CERT: DFN-CERT-2019-0112 CERT: DFN-CERT-2019-0104 CERT: DFN-CERT-2019-0103 CERT: DFN-CERT-2019-0102 CERT: DFN-CERT-2018-2541 CERT: DFN-CERT-2018-2539 CERT: DFN-CERT-2018-2513 CERT: DFN-CERT-2018-2456 CERT: DFN-CERT-2018-2444 CERT: DFN-CERT-2018-2396 CERT: DFN-CERT-2018-2360 CERT: DFN-CERT-2018-2338 CERT: DFN-CERT-2018-2214 CERT: CB-K22/0045 CERT: CB-K20/0324 CERT: CB-K20/0136 CERT: CB-K19/1121 CERT: CB-K19/0696 CERT: CB-K19/0622 CERT: CB-K19/0615 CERT: CB-K19/0321 CERT: CB-K19/0320 CERT: CB-K19/0319 CERT: CB-K19/0318 CERT: CB-K19/0316 CERT: CB-K19/0314 CERT: CB-K19/0050 CERT: CB-K19/0044 CERT: CB-K18/1173 CERT: CB-K18/1065 CERT: CB-K18/1039 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 9 | **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) | | |
| **Detail** |  | | |
| **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 CERT: DFN-CERT-2022-0121 CERT: DFN-CERT-2022-0076 CERT: DFN-CERT-2022-0024 CERT: DFN-CERT-2021-2527 CERT: DFN-CERT-2021-2394 CERT: DFN-CERT-2021-2223 CERT: DFN-CERT-2021-2216 CERT: DFN-CERT-2021-2214 CERT: DFN-CERT-2021-2197 CERT: DFN-CERT-2021-2196 CERT: DFN-CERT-2021-2190 CERT: DFN-CERT-2021-2155 CERT: DFN-CERT-2021-2126 CERT: DFN-CERT-2021-1996 CERT: DFN-CERT-2021-1825 CERT: DFN-CERT-2021-1803 CERT: DFN-CERT-2021-1740 CERT: DFN-CERT-2021-1670 CERT: DFN-CERT-2021-1660 CERT: DFN-CERT-2021-1549 CERT: DFN-CERT-2021-1547 CERT: DFN-CERT-2021-1537 CERT: DFN-CERT-2021-1500 CERT: DFN-CERT-2021-1418 CERT: DFN-CERT-2021-1330 CERT: DFN-CERT-2021-1132 CERT: DFN-CERT-2021-1129 CERT: DFN-CERT-2021-1128 CERT: DFN-CERT-2021-1098 CERT: DFN-CERT-2021-1070 CERT: DFN-CERT-2021-1061 CERT: DFN-CERT-2021-0984 CERT: DFN-CERT-2021-0884 CERT: DFN-CERT-2021-0862 CERT: DFN-CERT-2021-0829 CERT: DFN-CERT-2021-0821 CERT: DFN-CERT-2021-0818 CERT: DFN-CERT-2021-0813 CERT: DFN-CERT-2021-0807 CERT: DFN-CERT-2021-0806 CERT: DFN-CERT-2021-0740 CERT: DFN-CERT-2021-0696 CERT: DFN-CERT-2021-0656 CERT: DFN-CERT-2021-0630 CERT: DFN-CERT-2021-0629 CERT: DFN-CERT-2021-0409 CERT: DFN-CERT-2021-0408 CERT: DFN-CERT-2021-0379 CERT: DFN-CERT-2021-0363 CERT: CB-K22/0061 CERT: CB-K21/1097 CERT: CB-K21/1095 CERT: CB-K21/1065 CERT: CB-K21/0785 CERT: CB-K21/0770 CERT: CB-K21/0573 CERT: CB-K21/0572 CERT: CB-K21/0565 CERT: CB-K21/0421 CERT: CB-K21/0412 CERT: CB-K21/0409 CERT: CB-K21/0389 CERT: CB-K21/0317 CERT: CB-K21/0185 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 10 | **Finding** | Oracle MySQL Server = 5.6.48 Security Update (cpujul2020) - Windows |
| **Severity** | **High** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **Detail** |  | | |
| **Solution** | Update to version 5.6.49 or later. | | |
| **Remark** | CVE: CVE-2020-1967 CVE: CVE-2020-14539 CVE: CVE-2020-14559 CERT: DFN-CERT-2021-2192 CERT: DFN-CERT-2021-0830 CERT: DFN-CERT-2021-0826 CERT: DFN-CERT-2021-0444 CERT: DFN-CERT-2021-0140 CERT: DFN-CERT-2020-2295 CERT: DFN-CERT-2020-2286 CERT: DFN-CERT-2020-2006 CERT: DFN-CERT-2020-1827 CERT: DFN-CERT-2020-1788 CERT: DFN-CERT-2020-1508 CERT: DFN-CERT-2020-0956 CERT: DFN-CERT-2020-0930 CERT: DFN-CERT-2020-0841 CERT: DFN-CERT-2020-0824 CERT: DFN-CERT-2020-0822 CERT: CB-K21/1088 CERT: CB-K21/0070 CERT: CB-K20/1023 CERT: CB-K20/1017 CERT: CB-K20/0711 CERT: CB-K20/0708 CERT: CB-K20/0357 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 11 | **Finding** | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection |
| **Severity** | **Medium** | **Port** | TCP: 443, 1129, 3031, 3389, 4300, 5989, 6101, 6301, 8444, 9080, 10102 |
| **Target** | 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), 172.28.135.223(3389), 172.28.136.118(1129, 3389), 172.28.136.153(443, 3389), 172.28.137.52(1129, 4300), 172.28.190.131(3389), 172.28.190.133(443, 1129, 3389) | | |
| **Detail** | The TLSv1.0 and TLSv1.1 protocols contain known cryptographic  flaws like:   - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)   - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy  Encryption (FREAK) | | |
| **Solution** | It is recommended to disable the deprecated TLSv1.0 and/or  TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more  information. | | |
| **Remark** | CVE: CVE-2011-3389 CVE: CVE-2015-0204 CERT: DFN-CERT-2020-0177 CERT: DFN-CERT-2020-0111 CERT: DFN-CERT-2019-0068 CERT: DFN-CERT-2018-1441 CERT: DFN-CERT-2018-1408 CERT: DFN-CERT-2016-1372 CERT: DFN-CERT-2016-1164 CERT: DFN-CERT-2016-0388 CERT: DFN-CERT-2015-1853 CERT: DFN-CERT-2015-1332 CERT: DFN-CERT-2015-0884 CERT: DFN-CERT-2015-0800 CERT: DFN-CERT-2015-0758 CERT: DFN-CERT-2015-0567 CERT: DFN-CERT-2015-0544 CERT: DFN-CERT-2015-0530 CERT: DFN-CERT-2015-0396 CERT: DFN-CERT-2015-0375 CERT: DFN-CERT-2015-0374 CERT: DFN-CERT-2015-0305 CERT: DFN-CERT-2015-0199 CERT: DFN-CERT-2015-0079 CERT: DFN-CERT-2015-0021 CERT: DFN-CERT-2014-1414 CERT: DFN-CERT-2013-1847 CERT: DFN-CERT-2013-1792 CERT: DFN-CERT-2012-1979 CERT: DFN-CERT-2012-1829 CERT: DFN-CERT-2012-1530 CERT: DFN-CERT-2012-1380 CERT: DFN-CERT-2012-1377 CERT: DFN-CERT-2012-1292 CERT: DFN-CERT-2012-1214 CERT: DFN-CERT-2012-1213 CERT: DFN-CERT-2012-1180 CERT: DFN-CERT-2012-1156 CERT: DFN-CERT-2012-1155 CERT: DFN-CERT-2012-1039 CERT: DFN-CERT-2012-0956 CERT: DFN-CERT-2012-0908 CERT: DFN-CERT-2012-0868 CERT: DFN-CERT-2012-0867 CERT: DFN-CERT-2012-0848 CERT: DFN-CERT-2012-0838 CERT: DFN-CERT-2012-0776 CERT: DFN-CERT-2012-0722 CERT: DFN-CERT-2012-0638 CERT: DFN-CERT-2012-0627 CERT: DFN-CERT-2012-0451 CERT: DFN-CERT-2012-0418 CERT: DFN-CERT-2012-0354 CERT: DFN-CERT-2012-0234 CERT: DFN-CERT-2012-0221 CERT: DFN-CERT-2012-0177 CERT: DFN-CERT-2012-0170 CERT: DFN-CERT-2012-0146 CERT: DFN-CERT-2012-0142 CERT: DFN-CERT-2012-0126 CERT: DFN-CERT-2012-0123 CERT: DFN-CERT-2012-0095 CERT: DFN-CERT-2012-0051 CERT: DFN-CERT-2012-0047 CERT: DFN-CERT-2012-0021 CERT: DFN-CERT-2011-1953 CERT: DFN-CERT-2011-1946 CERT: DFN-CERT-2011-1844 CERT: DFN-CERT-2011-1826 CERT: DFN-CERT-2011-1774 CERT: DFN-CERT-2011-1743 CERT: DFN-CERT-2011-1738 CERT: DFN-CERT-2011-1706 CERT: DFN-CERT-2011-1628 CERT: DFN-CERT-2011-1627 CERT: DFN-CERT-2011-1619 CERT: DFN-CERT-2011-1482 CERT: CB-K18/0799 CERT: CB-K16/1289 CERT: CB-K16/1096 CERT: CB-K15/1751 CERT: CB-K15/1266 CERT: CB-K15/0850 CERT: CB-K15/0764 CERT: CB-K15/0720 CERT: CB-K15/0548 CERT: CB-K15/0526 CERT: CB-K15/0509 CERT: CB-K15/0493 CERT: CB-K15/0384 CERT: CB-K15/0365 CERT: CB-K15/0364 CERT: CB-K15/0302 CERT: CB-K15/0192 CERT: CB-K15/0079 CERT: CB-K15/0016 CERT: CB-K14/1342 CERT: CB-K14/0231 CERT: CB-K13/0845 CERT: CB-K13/0796 CERT: CB-K13/0790 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 12 | **Finding** | SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) |
| **Severity** | **Medium** | **Port** | TCP: 443, 3031, 5989, 6101, 6301, 8091, 9080, 9090, 10102 |
| **Target** | 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) | | |
| **Detail** | The flaw exists because the remote SSL/TLS service does not  properly restrict client-initiated renegotiation within the SSL and TLS protocols.   Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but  both are in a DISPUTED state with the following rationale:   > It can also be argued that it is the responsibility of server deployments, not a security  library, to prevent or limit renegotiation when it is inappropriate within a specific environment.   Both CVEs are still kept in this VT as a reference to the origin of this flaw. | | |
| **Solution** | Users should contact their vendors for specific patch information.   A general solution is to remove/disable renegotiation capabilities altogether from/in the affected  SSL/TLS service. | | |
| **Remark** | CVE: CVE-2011-1473 CVE: CVE-2011-5094 CERT: DFN-CERT-2017-1013 CERT: DFN-CERT-2017-1012 CERT: DFN-CERT-2014-0809 CERT: DFN-CERT-2013-1928 CERT: DFN-CERT-2012-1112 CERT: CB-K17/0980 CERT: CB-K17/0979 CERT: CB-K14/0772 CERT: CB-K13/0915 CERT: CB-K13/0462 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 13 | **Finding** | Weak Encryption Algorithm(s) Supported (SSH) |
| **Severity** | **Medium** | **Port** | TCP: 22 |
| **Target** | 172.28.131.23(22), 172.28.131.24(22) | | |
| **Detail** | '- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit  keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour  (and RC4) has problems with weak keys, and should not be used anymore.   - The 'none' algorithm specifies that no encryption is to be done. Note that this method provides  no confidentiality protection, and it is NOT RECOMMENDED to use it.   - A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to  recover plaintext from a block of ciphertext. | | |
| **Solution** | Disable the reported weak encryption algorithm(s). | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 14 | **Finding** | Cleartext Transmission of Sensitive Information via HTTP |
| **Severity** | **Medium** | **Port** | TCP: 4848, 8001, 9200 |
| **Target** | 172.28.131.24(9200), 172.28.131.49(4848), 172.28.137.52(8001) | | |
| **Detail** |  | | |
| **Solution** | Enforce the transmission of sensitive data via an encrypted SSL/TLS connection.  Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before  allowing to input sensitive data into the mentioned functions. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 15 | **Finding** | SSL/TLS: Report Weak Cipher Suites |
| **Severity** | **Medium** | **Port** | TCP: 443, 3031, 3389 |
| **Target** | 172.28.131.24(3031), 172.28.131.105(3389), 172.28.131.108(3389), 172.28.135.223(3389), 172.28.136.153(443), 172.28.190.131(3389), 172.28.190.133(3389) | | |
| **Detail** | These rules are applied for the evaluation of the cryptographic  strength:   - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)   - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods  and therefore considered as weak (CVE-2015-4000)   - 1024 bit RSA authentication is considered to be insecure and therefore as weak   - Any cipher considered to be secure for only the next 10 years is considered as medium   - Any other cipher is considered as strong | | |
| **Solution** | The configuration of this services should be changed so  that it does not accept the listed weak cipher suites anymore.   Please see the references for more resources supporting you with this task. | | |
| **Remark** | CVE: CVE-2013-2566 CVE: CVE-2015-2808 CVE: CVE-2015-4000 CERT: DFN-CERT-2021-0775 CERT: DFN-CERT-2020-1561 CERT: DFN-CERT-2020-1276 CERT: DFN-CERT-2017-1821 CERT: DFN-CERT-2016-1692 CERT: DFN-CERT-2016-1648 CERT: DFN-CERT-2016-1168 CERT: DFN-CERT-2016-0665 CERT: DFN-CERT-2016-0642 CERT: DFN-CERT-2016-0184 CERT: DFN-CERT-2016-0135 CERT: DFN-CERT-2016-0101 CERT: DFN-CERT-2016-0035 CERT: DFN-CERT-2015-1853 CERT: DFN-CERT-2015-1679 CERT: DFN-CERT-2015-1632 CERT: DFN-CERT-2015-1608 CERT: DFN-CERT-2015-1542 CERT: DFN-CERT-2015-1518 CERT: DFN-CERT-2015-1406 CERT: DFN-CERT-2015-1341 CERT: DFN-CERT-2015-1194 CERT: DFN-CERT-2015-1144 CERT: DFN-CERT-2015-1113 CERT: DFN-CERT-2015-1078 CERT: DFN-CERT-2015-1067 CERT: DFN-CERT-2015-1038 CERT: DFN-CERT-2015-1016 CERT: DFN-CERT-2015-1012 CERT: DFN-CERT-2015-0980 CERT: DFN-CERT-2015-0977 CERT: DFN-CERT-2015-0976 CERT: DFN-CERT-2015-0960 CERT: DFN-CERT-2015-0956 CERT: DFN-CERT-2015-0944 CERT: DFN-CERT-2015-0937 CERT: DFN-CERT-2015-0925 CERT: DFN-CERT-2015-0884 CERT: DFN-CERT-2015-0881 CERT: DFN-CERT-2015-0879 CERT: DFN-CERT-2015-0866 CERT: DFN-CERT-2015-0844 CERT: DFN-CERT-2015-0800 CERT: DFN-CERT-2015-0737 CERT: DFN-CERT-2015-0696 CERT: DFN-CERT-2014-0977 CERT: CB-K21/0067 CERT: CB-K19/0812 CERT: CB-K17/1750 CERT: CB-K16/1593 CERT: CB-K16/1552 CERT: CB-K16/1102 CERT: CB-K16/0617 CERT: CB-K16/0599 CERT: CB-K16/0168 CERT: CB-K16/0121 CERT: CB-K16/0090 CERT: CB-K16/0030 CERT: CB-K15/1751 CERT: CB-K15/1591 CERT: CB-K15/1550 CERT: CB-K15/1517 CERT: CB-K15/1514 CERT: CB-K15/1464 CERT: CB-K15/1442 CERT: CB-K15/1334 CERT: CB-K15/1269 CERT: CB-K15/1136 CERT: CB-K15/1090 CERT: CB-K15/1059 CERT: CB-K15/1022 CERT: CB-K15/1015 CERT: CB-K15/0986 CERT: CB-K15/0964 CERT: CB-K15/0962 CERT: CB-K15/0932 CERT: CB-K15/0927 CERT: CB-K15/0926 CERT: CB-K15/0907 CERT: CB-K15/0901 CERT: CB-K15/0896 CERT: CB-K15/0889 CERT: CB-K15/0877 CERT: CB-K15/0850 CERT: CB-K15/0849 CERT: CB-K15/0834 CERT: CB-K15/0827 CERT: CB-K15/0802 CERT: CB-K15/0764 CERT: CB-K15/0733 CERT: CB-K15/0667 CERT: CB-K14/0935 CERT: CB-K13/0942 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 16 | **Finding** | SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability |
| **Severity** | **Medium** | **Port** | TCP: 3389, 8091, 8181, 9090, 10102 |
| **Target** | 172.28.131.24(8091, 9090), 172.28.131.49(8181, 10102), 172.28.131.108(3389), 172.28.135.223(3389), 172.28.190.131(3389), 172.28.190.133(3389) | | |
| **Detail** | The Diffie-Hellman group are some big numbers that are used as base for  the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size  of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really  powerful attackers like governments. | | |
| **Solution** | Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use  a 2048-bit or stronger Diffie-Hellman group (see the references).   For Apache Web Servers:  Beginning with version 2.4.7, mod\_ssl will use DH parameters which include primes with lengths of more than 1024 bits. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 17 | **Finding** | jQuery 1.9.0 XSS Vulnerability |
| **Severity** | **Medium** | **Port** | TCP: 8090, 8091 |
| **Target** | 172.28.131.24(8090, 8091) | | |
| **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 CERT: DFN-CERT-2020-0590 CERT: CB-K22/0045 CERT: CB-K18/1131 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 18 | **Finding** | SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits |
| **Severity** | **Medium** | **Port** | TCP: 443, 3031, 9090 |
| **Target** | 172.28.131.24(443, 3031, 9090) | | |
| **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.** | 19 | **Finding** | SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection |
| **Severity** | **Medium** | **Port** | TCP: 3031 |
| **Target** | 172.28.131.24(3031) | | |
| **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 CERT: DFN-CERT-2018-0096 CERT: DFN-CERT-2017-1238 CERT: DFN-CERT-2017-1236 CERT: DFN-CERT-2016-1929 CERT: DFN-CERT-2016-1527 CERT: DFN-CERT-2016-1468 CERT: DFN-CERT-2016-1216 CERT: DFN-CERT-2016-1174 CERT: DFN-CERT-2016-1168 CERT: DFN-CERT-2016-0884 CERT: DFN-CERT-2016-0841 CERT: DFN-CERT-2016-0644 CERT: DFN-CERT-2016-0642 CERT: DFN-CERT-2016-0496 CERT: DFN-CERT-2016-0495 CERT: DFN-CERT-2016-0465 CERT: DFN-CERT-2016-0459 CERT: DFN-CERT-2016-0453 CERT: DFN-CERT-2016-0451 CERT: DFN-CERT-2016-0415 CERT: DFN-CERT-2016-0403 CERT: DFN-CERT-2016-0388 CERT: DFN-CERT-2016-0360 CERT: DFN-CERT-2016-0359 CERT: DFN-CERT-2016-0357 CERT: DFN-CERT-2016-0171 CERT: DFN-CERT-2015-1431 CERT: DFN-CERT-2015-1075 CERT: DFN-CERT-2015-1026 CERT: DFN-CERT-2015-0664 CERT: DFN-CERT-2015-0548 CERT: DFN-CERT-2015-0404 CERT: DFN-CERT-2015-0396 CERT: DFN-CERT-2015-0259 CERT: DFN-CERT-2015-0254 CERT: DFN-CERT-2015-0245 CERT: DFN-CERT-2015-0118 CERT: DFN-CERT-2015-0114 CERT: DFN-CERT-2015-0083 CERT: DFN-CERT-2015-0082 CERT: DFN-CERT-2015-0081 CERT: DFN-CERT-2015-0076 CERT: DFN-CERT-2014-1717 CERT: DFN-CERT-2014-1680 CERT: DFN-CERT-2014-1632 CERT: DFN-CERT-2014-1564 CERT: DFN-CERT-2014-1542 CERT: DFN-CERT-2014-1414 CERT: DFN-CERT-2014-1366 CERT: DFN-CERT-2014-1354 CERT: CB-K18/0094 CERT: CB-K17/1198 CERT: CB-K17/1196 CERT: CB-K16/1828 CERT: CB-K16/1438 CERT: CB-K16/1384 CERT: CB-K16/1141 CERT: CB-K16/1107 CERT: CB-K16/1102 CERT: CB-K16/0792 CERT: CB-K16/0599 CERT: CB-K16/0597 CERT: CB-K16/0459 CERT: CB-K16/0456 CERT: CB-K16/0433 CERT: CB-K16/0424 CERT: CB-K16/0415 CERT: CB-K16/0413 CERT: CB-K16/0374 CERT: CB-K16/0367 CERT: CB-K16/0331 CERT: CB-K16/0329 CERT: CB-K16/0328 CERT: CB-K16/0156 CERT: CB-K15/1514 CERT: CB-K15/1358 CERT: CB-K15/1021 CERT: CB-K15/0972 CERT: CB-K15/0637 CERT: CB-K15/0590 CERT: CB-K15/0525 CERT: CB-K15/0393 CERT: CB-K15/0384 CERT: CB-K15/0287 CERT: CB-K15/0252 CERT: CB-K15/0246 CERT: CB-K15/0237 CERT: CB-K15/0118 CERT: CB-K15/0110 CERT: CB-K15/0108 CERT: CB-K15/0080 CERT: CB-K15/0078 CERT: CB-K15/0077 CERT: CB-K15/0075 CERT: CB-K14/1617 CERT: CB-K14/1581 CERT: CB-K14/1537 CERT: CB-K14/1479 CERT: CB-K14/1458 CERT: CB-K14/1342 CERT: CB-K14/1314 CERT: CB-K14/1313 CERT: CB-K14/1311 CERT: CB-K14/1304 CERT: CB-K14/1296 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 20 | **Finding** | SSL/TLS: Certificate Signed Using A Weak Signature Algorithm |
| **Severity** | **Medium** | **Port** | TCP: 3031 |
| **Target** | 172.28.131.24(3031) | | |
| **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.** | 21 | **Finding** | SSL/TLS: Certificate Expired |
| **Severity** | **Medium** | **Port** | TCP: 3031 |
| **Target** | 172.28.131.24(3031) | | |
| **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.** | 22 | **Finding** | DCE/RPC and MSRPC Services Enumeration Reporting |
| **Severity** | **Medium** | **Port** | TCP: 135 |
| **Target** | 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), 172.28.135.223(135), 172.28.136.118(135), 172.28.136.153(135), 172.28.190.131(135), 172.28.190.133(135) | | |
| **Detail** |  | | |
| **Solution** | Filter incoming traffic to this ports. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 23 | **Finding** | SSL/TLS: Report Anonymous Cipher Suites |
| **Severity** | **Medium** | **Port** | TCP: 6101, 6301 |
| **Target** | 172.28.131.102(6101, 6301) | | |
| **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 CERT: DFN-CERT-2014-0049 CERT: DFN-CERT-2012-0442 CERT: CB-K14/0058 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 24 | **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) | | |
| **Detail** |  | | |
| **Solution** | Update to version 5.6.51, 5.7.31, 8.0.18 or later. | | |
| **Remark** | CVE: CVE-2021-2001 CERT: DFN-CERT-2021-2155 CERT: DFN-CERT-2021-0810 CERT: DFN-CERT-2021-0131 CERT: CB-K21/0062 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 25 | **Finding** | Oracle Mysql Security Updates (oct2017-3236626) 04 - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **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 CERT: DFN-CERT-2019-1047 CERT: DFN-CERT-2018-1276 CERT: DFN-CERT-2018-1265 CERT: DFN-CERT-2018-0515 CERT: DFN-CERT-2018-0260 CERT: DFN-CERT-2018-0242 CERT: DFN-CERT-2017-2137 CERT: DFN-CERT-2017-1827 CERT: CB-K18/0480 CERT: CB-K18/0242 CERT: CB-K18/0224 CERT: CB-K17/2048 CERT: CB-K17/1748 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 26 | **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) | | |
| **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 CERT: DFN-CERT-2019-0775 CERT: CB-K19/0319 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 27 | **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) | | |
| **Detail** |  | | |
| **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 CERT: DFN-CERT-2021-2155 CERT: DFN-CERT-2021-0002 CERT: DFN-CERT-2020-2763 CERT: DFN-CERT-2020-2756 CERT: DFN-CERT-2020-2620 CERT: DFN-CERT-2020-2380 CERT: DFN-CERT-2020-2295 CERT: CB-K20/1066 CERT: CB-K20/1017 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 28 | **Finding** | Oracle Mysql Security Updates (apr2018-3678067) 04 - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **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 CERT: DFN-CERT-2019-1047 CERT: DFN-CERT-2018-1276 CERT: DFN-CERT-2018-1265 CERT: DFN-CERT-2018-0913 CERT: DFN-CERT-2018-0723 CERT: CB-K18/0608 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 29 | **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) | | |
| **Detail** |  | | |
| **Solution** | Update to version 5.6.51, 5.7.33, 8.0.23 or later. | | |
| **Remark** | CVE: CVE-2021-2022 CVE: CVE-2021-2060 CERT: DFN-CERT-2021-2155 CERT: DFN-CERT-2021-0131 CERT: CB-K21/0062 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 30 | **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) | | |
| **Detail** |  | | |
| **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 CERT: DFN-CERT-2020-2014 CERT: DFN-CERT-2020-1729 CERT: DFN-CERT-2020-0895 CERT: DFN-CERT-2020-0776 CERT: DFN-CERT-2020-0775 CERT: DFN-CERT-2020-0772 CERT: DFN-CERT-2020-0716 CERT: DFN-CERT-2020-0277 CERT: DFN-CERT-2020-0101 CERT: DFN-CERT-2020-0096 CERT: DFN-CERT-2020-0091 CERT: DFN-CERT-2020-0090 CERT: DFN-CERT-2019-2164 CERT: DFN-CERT-2019-2149 CERT: DFN-CERT-2019-1900 CERT: DFN-CERT-2019-1897 CERT: DFN-CERT-2019-1559 CERT: CB-K22/0045 CERT: CB-K20/1049 CERT: CB-K20/1016 CERT: CB-K20/0321 CERT: CB-K20/0318 CERT: CB-K20/0043 CERT: CB-K20/0038 CERT: CB-K20/0036 CERT: CB-K20/0028 CERT: CB-K19/1025 CERT: CB-K19/0919 CERT: CB-K19/0915 CERT: CB-K19/0808 CERT: CB-K19/0675 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 31 | **Finding** | Oracle Mysql Security Updates (jul2017-3236622) 03 - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **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 CERT: DFN-CERT-2018-1276 CERT: DFN-CERT-2018-0242 CERT: DFN-CERT-2017-1956 CERT: DFN-CERT-2017-1675 CERT: DFN-CERT-2017-1519 CERT: DFN-CERT-2017-1465 CERT: DFN-CERT-2017-1282 CERT: DFN-CERT-2017-1243 CERT: CB-K18/0224 CERT: CB-K17/1870 CERT: CB-K17/1604 CERT: CB-K17/1453 CERT: CB-K17/1401 CERT: CB-K17/1239 CERT: CB-K17/1205 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 32 | **Finding** | Oracle MySQL Backronym Vulnerability June16 (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **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 CERT: DFN-CERT-2016-1004 CERT: DFN-CERT-2015-1105 CERT: DFN-CERT-2015-1096 CERT: DFN-CERT-2015-1071 CERT: DFN-CERT-2015-1051 CERT: DFN-CERT-2015-1016 CERT: DFN-CERT-2015-0942 CERT: CB-K18/0871 CERT: CB-K16/0944 CERT: CB-K15/1045 CERT: CB-K15/1042 CERT: CB-K15/1020 CERT: CB-K15/0994 CERT: CB-K15/0964 CERT: CB-K15/0895 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 33 | **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) | | |
| **Detail** |  | | |
| **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 CERT: DFN-CERT-2022-0586 CERT: DFN-CERT-2022-0118 CERT: DFN-CERT-2022-0112 CERT: DFN-CERT-2022-0052 CERT: DFN-CERT-2021-2527 CERT: DFN-CERT-2021-1931 CERT: CB-K22/0316 CERT: CB-K22/0077 CERT: CB-K22/0062 CERT: CB-K22/0030 CERT: CB-K21/0991 CERT: CB-K21/0969 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 34 | **Finding** | Oracle Mysql Security Updates (jul2017-3236622) 02 - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **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 CERT: DFN-CERT-2018-1276 CERT: DFN-CERT-2018-0242 CERT: DFN-CERT-2017-1956 CERT: DFN-CERT-2017-1806 CERT: DFN-CERT-2017-1675 CERT: DFN-CERT-2017-1519 CERT: DFN-CERT-2017-1465 CERT: DFN-CERT-2017-1341 CERT: DFN-CERT-2017-1282 CERT: DFN-CERT-2017-1243 CERT: CB-K18/0224 CERT: CB-K17/1870 CERT: CB-K17/1732 CERT: CB-K17/1604 CERT: CB-K17/1453 CERT: CB-K17/1401 CERT: CB-K17/1298 CERT: CB-K17/1239 CERT: CB-K17/1205 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 35 | **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) | | |
| **Detail** |  | | |
| **Solution** | Update to version 5.7.31, 8.0.18 or later. | | |
| **Remark** | CVE: CVE-2021-2160 CERT: DFN-CERT-2021-0821 CERT: CB-K21/0421 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 36 | **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) | | |
| **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 CERT: DFN-CERT-2019-2149 CERT: CB-K19/0915 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 37 | **Finding** | Oracle MySQL Security Update (cpujul2018 - 04) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **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 CERT: DFN-CERT-2019-1614 CERT: DFN-CERT-2019-1588 CERT: DFN-CERT-2019-1152 CERT: DFN-CERT-2019-1047 CERT: DFN-CERT-2019-0484 CERT: DFN-CERT-2018-1649 CERT: DFN-CERT-2018-1402 CERT: CB-K18/0795 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 38 | **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) | | |
| **Detail** |  | | |
| **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 CERT: DFN-CERT-2022-0076 CERT: DFN-CERT-2022-0074 CERT: DFN-CERT-2021-2527 CERT: DFN-CERT-2021-2438 CERT: DFN-CERT-2021-2369 CERT: DFN-CERT-2021-2185 CERT: DFN-CERT-2021-2155 CERT: DFN-CERT-2021-1743 CERT: DFN-CERT-2021-1677 CERT: DFN-CERT-2021-1593 CERT: DFN-CERT-2021-1580 CERT: DFN-CERT-2021-1537 CERT: DFN-CERT-2021-1329 CERT: DFN-CERT-2021-1174 CERT: DFN-CERT-2021-1165 CERT: DFN-CERT-2021-1157 CERT: DFN-CERT-2021-1151 CERT: DFN-CERT-2021-1148 CERT: DFN-CERT-2021-1045 CERT: DFN-CERT-2019-2216 CERT: CB-K22/0044 CERT: CB-K21/0813 CERT: CB-K21/0770 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 39 | **Finding** | Oracle Mysql Security Updates (oct2017-3236626) 02 - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **Detail** | The flaw exists due to an error in  'Server: Optimizer' | | |
| **Solution** | Apply the patch from the referenced advisory. | | |
| **Remark** | CVE: CVE-2017-10378 CERT: DFN-CERT-2019-1047 CERT: DFN-CERT-2018-1276 CERT: DFN-CERT-2018-1265 CERT: DFN-CERT-2018-0515 CERT: DFN-CERT-2018-0260 CERT: DFN-CERT-2018-0242 CERT: DFN-CERT-2017-2137 CERT: DFN-CERT-2017-1827 CERT: CB-K18/0480 CERT: CB-K18/0242 CERT: CB-K18/0224 CERT: CB-K17/2048 CERT: CB-K17/1748 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 40 | **Finding** | Oracle Mysql Security Updates (jan2018-3236628) 02 - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **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 CERT: DFN-CERT-2019-1047 CERT: DFN-CERT-2018-1276 CERT: DFN-CERT-2018-1265 CERT: DFN-CERT-2018-0515 CERT: DFN-CERT-2018-0424 CERT: DFN-CERT-2018-0286 CERT: DFN-CERT-2018-0101 CERT: CB-K18/0480 CERT: CB-K18/0392 CERT: CB-K18/0265 CERT: CB-K18/0096 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 41 | **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) | | |
| **Detail** |  | | |
| **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 CERT: DFN-CERT-2022-0076 CERT: DFN-CERT-2021-2190 CERT: DFN-CERT-2021-2155 CERT: DFN-CERT-2021-2126 CERT: DFN-CERT-2021-1504 CERT: DFN-CERT-2021-1225 CERT: DFN-CERT-2021-0924 CERT: DFN-CERT-2021-0862 CERT: DFN-CERT-2021-0828 CERT: DFN-CERT-2021-0826 CERT: DFN-CERT-2021-0821 CERT: DFN-CERT-2021-0819 CERT: DFN-CERT-2021-0715 CERT: DFN-CERT-2021-0408 CERT: DFN-CERT-2021-0338 CERT: DFN-CERT-2021-0255 CERT: DFN-CERT-2021-0134 CERT: DFN-CERT-2021-0131 CERT: DFN-CERT-2021-0128 CERT: DFN-CERT-2021-0120 CERT: DFN-CERT-2021-0107 CERT: DFN-CERT-2021-0078 CERT: DFN-CERT-2021-0012 CERT: DFN-CERT-2020-2791 CERT: DFN-CERT-2020-2668 CERT: CB-K21/1065 CERT: CB-K21/0788 CERT: CB-K21/0615 CERT: CB-K21/0421 CERT: CB-K21/0111 CERT: CB-K21/0062 CERT: CB-K21/0006 CERT: CB-K20/1217 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 42 | **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) | | |
| **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 CERT: DFN-CERT-2020-0103 CERT: DFN-CERT-2019-2149 CERT: CB-K19/0915 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 43 | **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) | | |
| **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 CERT: DFN-CERT-2020-2620 CERT: DFN-CERT-2020-2180 CERT: DFN-CERT-2020-0658 CERT: DFN-CERT-2020-0517 CERT: DFN-CERT-2019-2695 CERT: DFN-CERT-2019-2656 CERT: DFN-CERT-2019-2300 CERT: DFN-CERT-2019-2008 CERT: DFN-CERT-2019-1713 CERT: DFN-CERT-2019-1683 CERT: DFN-CERT-2019-1568 CERT: DFN-CERT-2019-1453 CERT: CB-K19/0620 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 44 | **Finding** | Oracle MySQL Server = 5.6.46 Security Update (cpujan2020) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **Detail** |  | | |
| **Solution** | Update to version 5.6.47 or later. | | |
| **Remark** | CVE: CVE-2020-2579 CERT: DFN-CERT-2020-1827 CERT: DFN-CERT-2020-1078 CERT: DFN-CERT-2020-0096 CERT: CB-K20/0038 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 45 | **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) | | |
| **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 CERT: DFN-CERT-2020-2620 CERT: DFN-CERT-2020-2189 CERT: DFN-CERT-2020-2180 CERT: DFN-CERT-2020-0092 CERT: DFN-CERT-2020-0048 CERT: DFN-CERT-2019-2625 CERT: DFN-CERT-2019-2457 CERT: DFN-CERT-2019-2300 CERT: DFN-CERT-2019-2274 CERT: DFN-CERT-2019-2158 CERT: DFN-CERT-2019-2157 CERT: DFN-CERT-2019-2046 CERT: DFN-CERT-2019-2008 CERT: DFN-CERT-2019-1996 CERT: DFN-CERT-2019-1897 CERT: DFN-CERT-2019-1755 CERT: DFN-CERT-2019-1746 CERT: DFN-CERT-2019-1722 CERT: DFN-CERT-2019-1713 CERT: DFN-CERT-2019-1683 CERT: DFN-CERT-2019-1678 CERT: DFN-CERT-2019-1677 CERT: DFN-CERT-2019-1617 CERT: DFN-CERT-2019-1614 CERT: DFN-CERT-2019-1486 CERT: DFN-CERT-2019-1460 CERT: DFN-CERT-2019-1455 CERT: DFN-CERT-2019-1453 CERT: DFN-CERT-2019-1450 CERT: DFN-CERT-2019-1408 CERT: DFN-CERT-2019-1240 CERT: DFN-CERT-2019-0968 CERT: DFN-CERT-2019-0781 CERT: DFN-CERT-2019-0775 CERT: DFN-CERT-2019-0771 CERT: DFN-CERT-2019-0566 CERT: DFN-CERT-2019-0556 CERT: DFN-CERT-2019-0412 CERT: CB-K22/0045 CERT: CB-K20/0041 CERT: CB-K19/0911 CERT: CB-K19/0639 CERT: CB-K19/0623 CERT: CB-K19/0622 CERT: CB-K19/0620 CERT: CB-K19/0619 CERT: CB-K19/0615 CERT: CB-K19/0332 CERT: CB-K19/0320 CERT: CB-K19/0319 CERT: CB-K19/0173 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 46 | **Finding** | Oracle MySQL Server = 5.7.33 Security Update (cpuapr2021) - Windows |
| **Severity** | **Medium** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **Detail** |  | | |
| **Solution** | Update to version 5.7.34 or later. | | |
| **Remark** | CVE: CVE-2021-2154 CERT: DFN-CERT-2021-1660 CERT: DFN-CERT-2021-0984 CERT: DFN-CERT-2021-0821 CERT: CB-K21/0421 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 47 | **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) | | |
| **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 CERT: DFN-CERT-2020-2763 CERT: DFN-CERT-2020-2756 CERT: DFN-CERT-2020-2620 CERT: DFN-CERT-2020-2299 CERT: DFN-CERT-2020-2180 CERT: DFN-CERT-2020-1827 CERT: DFN-CERT-2020-0658 CERT: DFN-CERT-2020-0517 CERT: DFN-CERT-2020-0103 CERT: DFN-CERT-2019-2695 CERT: DFN-CERT-2019-2687 CERT: DFN-CERT-2019-2656 CERT: DFN-CERT-2019-2301 CERT: DFN-CERT-2019-2149 CERT: CB-K20/1030 CERT: CB-K20/0109 CERT: CB-K19/0915 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 48 | **Finding** | VNC Server Unencrypted Data Transmission |
| **Severity** | **Medium** | **Port** | TCP: 5900 |
| **Target** | 172.28.135.223(5900) | | |
| **Detail** |  | | |
| **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.** | 49 | **Finding** | SMTP Server on non standard port |
| **Severity** | **Medium** | **Port** | TCP: 25000 |
| **Target** | 172.28.137.52(25000) | | |
| **Detail** |  | | |
| **Solution** | Check and clean your configuration. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 50 | **Finding** | Weak Host Key Algorithm(s) (SSH) |
| **Severity** | **Medium** | **Port** | TCP: 22 |
| **Target** | 172.28.137.52(22) | | |
| **Detail** |  | | |
| **Solution** | Disable the reported weak host key algorithm(s). | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 51 | **Finding** | Missing `httpOnly` Cookie Attribute |
| **Severity** | **Medium** | **Port** | TCP: 8081 |
| **Target** | 172.28.137.52(8081) | | |
| **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.** | 52 | **Finding** | TCP timestamps |
| **Severity** | **Low** | **Port** | TCP: 0 |
| **Target** | 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), 172.28.135.223(0), 172.28.136.118(0), 172.28.136.153(0), 172.28.190.131(0), 172.28.190.133(0) | | |
| **Detail** | The remote host implements TCP timestamps, as defined by RFC1323/RFC7323. | | |
| **Solution** | To disable TCP timestamps on linux add the line 'net.ipv4.tcp\_timestamps = 0' to  /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.   To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'   Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.   The default behavior of the TCP/IP stack on this Systems is to not use the  Timestamp options when initiating TCP connections, but use them if the TCP peer  that is initiating communication includes them in their synchronize (SYN) segment.   See the references for more information. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 53 | **Finding** | SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) |
| **Severity** | **Low** | **Port** | TCP: 3031 |
| **Target** | 172.28.131.24(3031) | | |
| **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 CERT: DFN-CERT-2017-1238 CERT: DFN-CERT-2017-1236 CERT: DFN-CERT-2016-1929 CERT: DFN-CERT-2016-1527 CERT: DFN-CERT-2016-1468 CERT: DFN-CERT-2016-1168 CERT: DFN-CERT-2016-0884 CERT: DFN-CERT-2016-0642 CERT: DFN-CERT-2016-0388 CERT: DFN-CERT-2016-0171 CERT: DFN-CERT-2015-1431 CERT: DFN-CERT-2015-1075 CERT: DFN-CERT-2015-1026 CERT: DFN-CERT-2015-0664 CERT: DFN-CERT-2015-0548 CERT: DFN-CERT-2015-0404 CERT: DFN-CERT-2015-0396 CERT: DFN-CERT-2015-0259 CERT: DFN-CERT-2015-0254 CERT: DFN-CERT-2015-0245 CERT: DFN-CERT-2015-0118 CERT: DFN-CERT-2015-0114 CERT: DFN-CERT-2015-0083 CERT: DFN-CERT-2015-0082 CERT: DFN-CERT-2015-0081 CERT: DFN-CERT-2015-0076 CERT: DFN-CERT-2014-1717 CERT: DFN-CERT-2014-1680 CERT: DFN-CERT-2014-1632 CERT: DFN-CERT-2014-1564 CERT: DFN-CERT-2014-1542 CERT: DFN-CERT-2014-1414 CERT: DFN-CERT-2014-1366 CERT: DFN-CERT-2014-1354 CERT: CB-K17/1198 CERT: CB-K17/1196 CERT: CB-K16/1828 CERT: CB-K16/1438 CERT: CB-K16/1384 CERT: CB-K16/1102 CERT: CB-K16/0599 CERT: CB-K16/0156 CERT: CB-K15/1514 CERT: CB-K15/1358 CERT: CB-K15/1021 CERT: CB-K15/0972 CERT: CB-K15/0637 CERT: CB-K15/0590 CERT: CB-K15/0525 CERT: CB-K15/0393 CERT: CB-K15/0384 CERT: CB-K15/0287 CERT: CB-K15/0252 CERT: CB-K15/0246 CERT: CB-K15/0237 CERT: CB-K15/0118 CERT: CB-K15/0110 CERT: CB-K15/0108 CERT: CB-K15/0080 CERT: CB-K15/0078 CERT: CB-K15/0077 CERT: CB-K15/0075 CERT: CB-K14/1617 CERT: CB-K14/1581 CERT: CB-K14/1537 CERT: CB-K14/1479 CERT: CB-K14/1458 CERT: CB-K14/1342 CERT: CB-K14/1314 CERT: CB-K14/1313 CERT: CB-K14/1311 CERT: CB-K14/1304 CERT: CB-K14/1296 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 54 | **Finding** | Oracle MySQL Security Update (cpujul2018 - 02) - Windows |
| **Severity** | **Low** | **Port** | TCP: 3307 |
| **Target** | 172.28.131.108(3307) | | |
| **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 CERT: DFN-CERT-2019-1614 CERT: DFN-CERT-2019-1588 CERT: DFN-CERT-2019-1152 CERT: DFN-CERT-2019-1047 CERT: DFN-CERT-2019-0484 CERT: DFN-CERT-2019-0112 CERT: DFN-CERT-2018-1649 CERT: DFN-CERT-2018-1402 CERT: DFN-CERT-2018-1276 CERT: DFN-CERT-2018-0913 CERT: CB-K18/0795 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 55 | **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) | | |
| **Detail** |  | | |
| **Solution** | Update to version 5.6.45, 5.7.19 or later. | | |
| **Remark** | CVE: CVE-2019-2730 CERT: DFN-CERT-2019-2169 CERT: DFN-CERT-2019-1453 CERT: CB-K19/0620 | | |



# Appendix

## **6.1 About Nessus**

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

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

### **6.1.1 Nessus vulnerabilities**

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

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

### **6.1.2 Nessus risk score**

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

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

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

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

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

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

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

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

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