**Vulnerability Assessment Report**

**For**



**SPIH phase 3 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 |

|  |  |  |  |
| --- | --- | --- | --- |
| SPIH phase 3 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 | - | 172.28.136.111 | 0 | 0 | 5 | 1 | 6 |
| 2 | - | 172.28.136.141 | 0 | 0 | 3 | 0 | 3 |
| 3 | - | 172.28.137.112 | 0 | 2 | 12 | 1 | 15 |
| **Total** | | | 0 | 2 | 20 | 2 | 24 |

## **5.3 Infrastructure Vulnerability Detail**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 1 | **Finding** | OpenSSH Multiple Vulnerabilities Jan17 (Windows) |
| **Severity** | **High** | **Port** | TCP: 22 |
| **Target** | 172.28.137.112(22) | | |
| **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 CERT: DFN-CERT-2021-0776 CERT: DFN-CERT-2019-1408 CERT: DFN-CERT-2018-2259 CERT: DFN-CERT-2018-2191 CERT: DFN-CERT-2018-2068 CERT: DFN-CERT-2018-1828 CERT: DFN-CERT-2018-1568 CERT: DFN-CERT-2018-1432 CERT: DFN-CERT-2018-1112 CERT: DFN-CERT-2018-1070 CERT: DFN-CERT-2018-1068 CERT: DFN-CERT-2018-0150 CERT: DFN-CERT-2018-0046 CERT: DFN-CERT-2017-2320 CERT: DFN-CERT-2017-2208 CERT: DFN-CERT-2017-1340 CERT: DFN-CERT-2017-1096 CERT: DFN-CERT-2017-0532 CERT: DFN-CERT-2017-0386 CERT: DFN-CERT-2017-0130 CERT: DFN-CERT-2017-0042 CERT: DFN-CERT-2016-2099 CERT: CB-K18/0919 CERT: CB-K18/0591 CERT: CB-K18/0137 CERT: CB-K18/0041 CERT: CB-K17/2219 CERT: CB-K17/2112 CERT: CB-K17/1292 CERT: CB-K17/1061 CERT: CB-K17/0527 CERT: CB-K17/0377 CERT: CB-K17/0127 CERT: CB-K17/0041 CERT: CB-K16/1991 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 2 | **Finding** | OpenSSH Denial of Service And User Enumeration Vulnerabilities (Windows) |
| **Severity** | **High** | **Port** | TCP: 22 |
| **Target** | 172.28.137.112(22) | | |
| **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 CERT: DFN-CERT-2019-1408 CERT: DFN-CERT-2018-1828 CERT: DFN-CERT-2018-1070 CERT: DFN-CERT-2018-0046 CERT: DFN-CERT-2017-2320 CERT: DFN-CERT-2017-2208 CERT: DFN-CERT-2017-1831 CERT: DFN-CERT-2017-1407 CERT: DFN-CERT-2017-1340 CERT: DFN-CERT-2017-0060 CERT: DFN-CERT-2016-1943 CERT: DFN-CERT-2016-1729 CERT: DFN-CERT-2016-1576 CERT: DFN-CERT-2016-1574 CERT: DFN-CERT-2016-1331 CERT: DFN-CERT-2016-1243 CERT: DFN-CERT-2016-1149 CERT: CB-K18/0041 CERT: CB-K17/2219 CERT: CB-K17/2112 CERT: CB-K17/1753 CERT: CB-K17/1349 CERT: CB-K17/1292 CERT: CB-K17/0055 CERT: CB-K16/1837 CERT: CB-K16/1629 CERT: CB-K16/1487 CERT: CB-K16/1485 CERT: CB-K16/1252 CERT: CB-K16/1221 CERT: CB-K16/1082 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 3 | **Finding** | SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability |
| **Severity** | **Medium** | **Port** | TCP: 3389, 7630 |
| **Target** | 172.28.136.111(3389), 172.28.137.112(7630) | | |
| **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.** | 4 | **Finding** | SSL/TLS: Report Weak Cipher Suites |
| **Severity** | **Medium** | **Port** | TCP: 3389 |
| **Target** | 172.28.136.111(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.** | 5 | **Finding** | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection |
| **Severity** | **Medium** | **Port** | TCP: 1129, 3389, 4316, 7630 |
| **Target** | 172.28.136.111(1129, 3389), 172.28.136.141(1129, 3389), 172.28.137.112(1129, 4316, 7630) | | |
| **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.** | 6 | **Finding** | DCE/RPC and MSRPC Services Enumeration Reporting |
| **Severity** | **Medium** | **Port** | TCP: 135 |
| **Target** | 172.28.136.111(135), 172.28.136.141(135) | | |
| **Detail** |  | | |
| **Solution** | Filter incoming traffic to this ports. | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 7 | **Finding** | Weak Host Key Algorithm(s) (SSH) |
| **Severity** | **Medium** | **Port** | TCP: 22 |
| **Target** | 172.28.137.112(22) | | |
| **Detail** |  | | |
| **Solution** | Disable the reported weak host key algorithm(s). | | |
| **Remark** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 8 | **Finding** | SSL/TLS: Certificate Expired |
| **Severity** | **Medium** | **Port** | TCP: 7630 |
| **Target** | 172.28.137.112(7630) | | |
| **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.** | 9 | **Finding** | OpenSSH sftp-server Security Bypass Vulnerability (Windows) |
| **Severity** | **Medium** | **Port** | TCP: 22 |
| **Target** | 172.28.137.112(22) | | |
| **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 CERT: DFN-CERT-2019-0362 CERT: DFN-CERT-2018-2554 CERT: DFN-CERT-2018-2191 CERT: DFN-CERT-2018-2068 CERT: DFN-CERT-2018-1828 CERT: DFN-CERT-2018-1568 CERT: DFN-CERT-2018-0150 CERT: DFN-CERT-2017-2217 CERT: DFN-CERT-2017-2100 CERT: DFN-CERT-2017-2093 CERT: CB-K20/0041 CERT: CB-K18/0137 CERT: CB-K17/2126 CERT: CB-K17/2014 CERT: CB-K17/2002 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 10 | **Finding** | SSL/TLS: Missing `secure` Cookie Attribute |
| **Severity** | **Medium** | **Port** | TCP: 7630 |
| **Target** | 172.28.137.112(7630) | | |
| **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.** | 11 | **Finding** | OpenSSH 7.8 User Enumeration Vulnerability - Windows |
| **Severity** | **Medium** | **Port** | TCP: 22 |
| **Target** | 172.28.137.112(22) | | |
| **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 CERT: DFN-CERT-2021-2178 CERT: DFN-CERT-2020-2189 CERT: DFN-CERT-2020-0228 CERT: DFN-CERT-2019-2046 CERT: DFN-CERT-2019-0857 CERT: DFN-CERT-2019-0362 CERT: DFN-CERT-2018-2293 CERT: DFN-CERT-2018-2259 CERT: DFN-CERT-2018-2191 CERT: DFN-CERT-2018-1806 CERT: DFN-CERT-2018-1696 CERT: CB-K20/0041 CERT: CB-K18/1031 CERT: CB-K18/0873 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 12 | **Finding** | OpenSSH auth2-gss.c User Enumeration Vulnerability - Windows |
| **Severity** | **Medium** | **Port** | TCP: 22 |
| **Target** | 172.28.137.112(22) | | |
| **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 CERT: DFN-CERT-2018-2293 CERT: DFN-CERT-2018-2191 CERT: CB-K18/0885 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 13 | **Finding** | Missing `httpOnly` Cookie Attribute |
| **Severity** | **Medium** | **Port** | TCP: 7630 |
| **Target** | 172.28.137.112(7630) | | |
| **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.** | 14 | **Finding** | SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) |
| **Severity** | **Medium** | **Port** | TCP: 7630 |
| **Target** | 172.28.137.112(7630) | | |
| **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.** | 15 | **Finding** | TCP timestamps |
| **Severity** | **Low** | **Port** | TCP: 0 |
| **Target** | 172.28.136.111(0), 172.28.137.112(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** |  | | |



# 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. |