**Vulnerability Assessment Report**

**For**



**Health Care Cloud**

**Date March 03 2022**

**Document Security Level:** Confidential

**Document Version:** 1.0

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

|  |  |  |  |
| --- | --- | --- | --- |
| Health Care Cloud | | 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](#_Toc97201647)

[2. Operation Method 5](#_Toc97201648)

[3. Project Scope 6](#_Toc97201649)

[3.1 Infrastructure Vulnerability Assessment 6](#_Toc97201650)

[3.2 Web Application Vulnerability Assessment 6](#_Toc97201651)

[4. Testing Tools 7](#_Toc97201652)

[5. Infrastructure Vulnerability Assessment 7](#_Toc97201653)

[5.1 Target Information 8](#_Toc97201654)

[5.2 Executive summary 9](#_Toc97201655)

[5.2.1 Summary Vulnerability by Severity 9](#_Toc97201656)

[5.2.2 Vulnerability by Target 9](#_Toc97201657)

[5.3 Infrastructure Vulnerability Detail 11](#_Toc97201658)

[6. Web Application Vulnerability Assessment 12](#_Toc97201659)

[6.1 Target Information 13](#_Toc97201660)

[6.2 Executive summary 14](#_Toc97201661)

[6.2.1 Summary Vulnerability by Severity 14](#_Toc97201662)

[6.2.2 Vulnerability by Target 14](#_Toc97201663)

[6.3 Web Application Vulnerability Detail 15](#_Toc97201664)

[7. Port Discovery 18](#_Toc97201665)

[8. Appendix 19](#_Toc97201666)

[8.1 About Nessus 19](#_Toc97201667)

[8.1.1 Nessus vulnerabilities 19](#_Toc97201668)

[8.1.2 Nessus risk score 19](#_Toc97201669)

[8.2 About Acunetix 21](#_Toc97201670)

[8.2.1 Acunetix web vulnerabilities 21](#_Toc97201671)

[8.2.2 Acunetix risk score 22](#_Toc97201672)

# 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 | DATABASE01 | - | 172.16.69.13 | Ubuntu 18 | Database Server 01 |  | ✓ |
| 2 | WEB01 | 123.123.123.123 | 172.16.69.14 | Ubuntu 20 | Web Server |  | ✓ |
| 3 | TERM | - | 172.16.69.52 | Windows Server 2016 | Terminal Server |  | ✓ |
| 4 | SMB01 | 12.12.12.12 | 172.16.69.53 | Windows Server 2019 | SMB Server |  | ✓ |
| 5 | DATABASE02 | - | 172.16.69.54 | Ubuntu 18 | Database Server 02 |  | ✓ |

## **3.2 Web Application Vulnerability Assessment**

**Target / IP Address:**

| **No.** | **Domain / Server Name** | **Public IP Address** | **Private IP Address** | **OS/Model** | **Functions** | **Public Assessment** | **Private Assessment** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | https://example.com/ | 123.123.123.123 | 172.16.69.14 | Ubuntu 20 | เว็บไซต์ขายของ | ✓ |  |

# Testing Tools

|  |  |
| --- | --- |
| **Tool Name** | **Testing Type** |
| Nmap | Host and Service Discovery |
| Nessus | Infrastructure Vulnerability Assessment |
| Acunetix | Web Application Vulnerability Assessment |

# Infrastructure Vulnerability Assessment

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

**Testing date:** March 30, 2021

**Tester IP Address:** 203.150.110.29

Diagram

Description automatically generated

Figure 2: Vulnerability Assessment from Public Access

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

**Testing date:** March 30, 2021

**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 |  | 10.20.201.101 |  | TCP : 22, 111, 443, 5060 UDP : 111 |
| 2 |  | 10.20.202.11 |  | TCP : 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 3 |  | 10.20.202.12 |  | TCP : 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 4 |  | 10.20.202.13 |  | TCP : 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 5 |  | 10.20.202.14 |  | TCP : 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 6 |  | 10.20.202.15 |  | TCP : 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 7 |  | 10.20.202.16 |  | TCP : 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 8 |  | 10.20.202.101 |  | TCP : 53, 88, 135, 139, 389, 445, 464, 593, 636, 2000, 3269, 3389, 5060, 5985, 49152, 49155, 49159, 49166, 49175, 49178, 49209 UDP : 53 |
| 9 |  | 10.20.202.103 |  | TCP : 80, 88, 135, 139, 389, 443, 445, 636, 2000, 2012, 2014, 2015, 2020, 3389, 5060, 5985, 7080, 8900 |
| 10 |  | 10.20.202.104 |  | TCP : 135, 139, 445, 2000, 3389, 5060, 5985, 49152, 49153, 49154, 49155, 49169, 49172, 49179, 49180, 49185 UDP : 1434 |
| 11 |  | 10.20.202.105 |  | TCP : 80, 135, 139, 443, 445, 514, 1514, 2000, 2020, 3389, 5060, 5985, 6501, 6502, 8900, 9443, 49152, 49153, 49154, 49155, 49156, 49172, 49187, 49189 |
| 12 |  | 10.20.202.137 |  | TCP : 135, 139, 445, 3389, 5060, 5985, 49152, 49153, 49154, 49155, 49167, 49172, 49182, 49183 |
| 13 |  | 10.20.202.138 |  | TCP : 135, 139, 445, 1433, 2000, 3389, 5060, 49152, 49153, 49154, 49155, 49167, 49172, 49186, 49187 UDP : 1434 |
| 14 |  | 10.20.202.140 |  | TCP : 135, 139, 445, 2000, 3389, 5060, 5985, 49152, 49153, 49154, 49155, 49156, 49158, 49159 |
| 15 |  | 10.20.202.141 |  | TCP : 135, 139, 445, 2000, 3389, 5060, 5985, 49664, 49665, 49666, 49667, 49668, 49669 |
| 16 |  | 10.20.202.151 |  | TCP : 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 17 |  | 10.20.202.152 |  | TCP : 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 18 |  | 10.20.202.153 |  | TCP : 80, 427, 443, 902, 2000, 5060, 8000, 8182, 8300 |
| 19 |  | 10.20.202.154 |  | TCP : 2, 5, 11, 33, 39, 55, 58, 61, 64, 67, 80, 83, 86, 89, 92, 108, 111, 114, 117, 120, 136, 139, 142, 145, 161, 164, 167, 170, 173, 189, 192, 195, 198, 214, 217, 220, 223, 242, 245, 248, 267, 320, 348, 351, 354, 357, 376, 379, 382, 385, 401, 404, 407, 410, 427, 429, 432, 435, 438, 443, 454, 457, 460, 463, 482, 485, 488, 491, 507, 510, 513, 516, 535, 538, 541, 544, 560, 563, 566, 569, 588, 591, 594, 597, 613, 616, 619, 622, 641, 644, 647, 650, 666, 669, 672, 675, 694, 697, 700, 747, 750, 753, 772, 775, 781, 800, 828, 887, 902, 912, 990, 993, 1040, 1065, 1068, 1071, 1074, 1090, 1093, 1096, 1099, 1124, 1127, 1180, 1199, 1202, 1205, 1224, 1227, 1230, 1233, 1249, 1252, 1255, 1258, 1277, 1280, 1283, 1286, 1302, 1305, 1308, 1311, 1330, 1333, 1336, 1339, 1355, 1358, 1361, 1364, 1383, 1386, 1389, 1392, 1408, 1411, 1414, 1417, 1436, 1439, 1442, 1445, 1461, 1464, 1467, 1470, 1489, 1492, 1495, 1498, 1514, 1517, 1520, 1523, 1542, 1545, 1548, 1551, 1567, 1570, 1573, 1576, 1595, 1598, 1601, 1604, 1620, 1623, 1626, 1629, 1648, 1651, 1654, 1657, 1673, 1676, 1679, 1682, 1701, 1704, 1707, 1710, 1726, 1729, 1732, 1735, 1754, 1757, 1760, 1763, 1779, 1782, 1785, 1788, 1807, 1810, 1813, 1816, 1832, 1835, 1838, 1841, 1860, 1863, 1866, 1869, 1885, 1888, 1891, 1894, 1913, 1916, 1919, 1922, 1938, 1941, 1944, 1947, 1966, 1969, 1972, 1975, 1991, 1994, 1997, 2000, 2019, 2022, 2025, 2028, 2044, 2047, 2050, 2053, 2072, 2075, 2078, 2081, 2097, 2100, 2103, 2106, 2125, 2128, 2131, 2134, 2150, 2159, 2181, 2234, 2237, 2240, 2284, 2287, 2309, 2315, 2318, 2337, 2340, 2343, 2346, 2362, 2365, 2368, 2371, 2390, 2393, 2396, 2399, 2415, 2418, 2421, 2424, 2443, 2446, 2449, 2452, 2468, 2471, 2474, 2477, 2496, 2499, 2502, 2505, 2521, 2524, 2527, 2530, 2549, 2552, 2555, 2558, 2574, 2577, 2580, 2583, 2602, 2605, 2608, 2611, 2627, 2630, 2633, 2636, 2655, 2658, 2661, 2664, 2680, 2683, 2686, 2689, 2708, 2711, 2714, 2717, 2733, 2736, 2739, 2742, 2761, 2764, 2767, 2770, 2786, 2789, 2792, 2795, 2814, 2817, 2820, 2823, 2839, 2842, 2845, 2848, 2867, 2870, 2873, 2876, 2892, 2895, 2898, 2901, 2920, 2923, 2926, 2929, 2945, 2948, 2951, 2954, 2973, 2976, 2979, 2982, 2998, 3001, 3004, 3007, 3026, 3029, 3032, 3035, 3051, 3054, 3057, 3060, 3079, 3082, 3085, 3088, 3104, 3107, 3110, 3113, 3132, 3135, 3138, 3141, 3157, 3160, 3163, 3166, 3185, 3188, 3191, 3194, 3210, 3213, 3216, 3219, 3238, 3241, 3244, 3247, 3263, 3266, 3269, 3272, 3291, 3294, 3297, 3316, 3319, 3344, 3347, 3350, 3353, 3372, 3375, 3378, 3397, 3400, 3403, 3406, 3422, 3425, 3428, 3431, 3450, 3453, 3456, 3459, 3475, 3478, 3481, 3484, 3503, 3506, 3509, 3512, 3528, 3531, 3534, 3537, 3556, 3559, 3562, 3565, 3581, 3584, 3587, 3590, 3609, 3612, 3615, 3618, 3634, 3637, 3640, 3643, 3662, 3665, 3668, 3671, 3687, 3690, 3693, 3696, 3715, 3718, 3721, 3724, 3740, 3743, 3746, 3749, 3768, 3774, 3777, 3793, 3796, 3799, 3802, 3846, 3849, 3852, 3855, 3986, 4005, 4008, 4011, 4014, 4033, 4036, 4042, 4111, 4114, 4142, 4145, 4201, 4351, 4354, 4357, 4457, 4569, 4672, 4800, 4837, 4987, 5021, 5060, 5065, 5071, 5093, 5099, 5102, 5152, 5177, 5202, 5305, 5308, 5311, 5314, 5411, 5414, 5417, 5420, 5520, 5595, 5598, 5601, 5604, 5632, 5676, 5679, 5729, 5757, 5813, 5888, 5969, 5989, 5997, 6000, 6003, 6050, 6072, 6100, 6103, 6106, 6109, 6321, 6343, 6346, 6443, 6471, 6502, 6505, 6549, 6558, 6580, 6714, 6767, 6789, 6842, 6901, 7001, 7004, 7007, 7010, 7269, 7300, 7428, 7431, 7743, 7777, 7902, 7933, 7955, 7980, 8000, 8008, 8033, 8089, 8123, 8182, 8192, 8201, 8245, 8300, 8351, 8379, 8834, 8887, 8890, 8987, 9021, 9024, 9043, 9080, 9099, 9102, 9152, 9202, 9205, 9283, 9392, 9495, 9704, 9872, 9888, 9950, 9994, 9997, 10000, 10003, 10081, 10103, 10128, 11001, 11319, 12223, 12753, 13710, 13713, 13819, 14034, 14237, 15858, 16360, 18000, 18184, 18187, 18190, 19191, 19194, 19412, 19540, 20011, 20020, 20999, 21071, 21317, 21554, 21847, 22000, 22003, 22321, 22555, 23456, 23945, 24678, 25002, 25005, 25903, 26000, 27007, 27010, 28017, 31300, 31337, 31786, 32123, 32768, 32787, 32896, 33270, 34012, 34249, 34324, 34567, 36079, 36865, 38037, 40001, 40843, 41002, 41080, 41111, 41794, 44322, 44818, 47000, 47624, 48001, 48556, 61441, 65301 |
| 20 |  | 10.20.202.155 |  | TCP : 1, 4, 29, 54, 57, 79, 80, 82, 107, 110, 132, 160, 163, 185, 188, 213, 216, 266, 319, 322, 344, 347, 372, 375, 397, 400, 425, 427, 428, 443, 450, 453, 478, 481, 503, 506, 531, 534, 556, 559, 584, 587, 609, 612, 637, 640, 662, 665, 690, 693, 771, 799, 902, 1008, 1036, 1061, 1064, 1089, 1114, 1117, 1170, 1220, 1223, 1248, 1273, 1276, 1301, 1326, 1329, 1354, 1379, 1382, 1407, 1432, 1435, 1460, 1485, 1488, 1513, 1538, 1541, 1566, 1591, 1594, 1619, 1644, 1647, 1672, 1697, 1700, 1725, 1750, 1753, 1778, 1803, 1806, 1831, 1856, 1859, 1884, 1909, 1912, 1937, 1962, 1965, 1990, 2000, 2015, 2018, 2043, 2068, 2071, 2096, 2121, 2124, 2149, 2174, 2177, 2202, 2255, 2280, 2283, 2308, 2333, 2336, 2361, 2386, 2389, 2414, 2439, 2442, 2467, 2470, 2492, 2495, 2520, 2523, 2545, 2548, 2573, 2576, 2598, 2601, 2626, 2629, 2651, 2654, 2679, 2704, 2707, 2732, 2735, 2757, 2760, 2785, 2788, 2810, 2813, 2838, 2841, 2863, 2866, 2891, 2894, 2916, 2919, 2944, 2947, 2969, 2972, 2997, 3000, 3022, 3025, 3050, 3053, 3075, 3078, 3103, 3106, 3128, 3131, 3156, 3159, 3181, 3184, 3209, 3212, 3234, 3237, 3262, 3265, 3287, 3290, 3315, 3318, 3340, 3343, 3393, 3396, 3421, 3424, 3446, 3449, 3474, 3477, 3499, 3502, 3527, 3530, 3552, 3555, 3580, 3583, 3605, 3608, 3633, 3636, 3658, 3661, 3686, 3689, 3711, 3714, 3739, 3742, 3764, 3767, 3792, 3795, 3845, 3848, 3870, 4004, 4007, 4029, 4032, 4138, 4347, 4350, 4400, 4453, 4456, 4559, 4802, 4827, 4983, 5011, 5060, 5064, 5145, 5226, 5251, 5301, 5304, 5354, 5407, 5410, 5435, 5463, 5566, 5569, 5597, 5675, 5859, 5968, 5989, 5990, 6071, 6149, 6177, 6255, 6389, 6548, 6788, 6841, 6891, 7000, 7505, 7580, 7633, 7845, 7979, 8000, 8004, 8007, 8032, 8060, 8088, 8182, 8191, 8194, 8216, 8300, 8378, 8403, 8431, 8484, 8880, 8989, 9080, 9201, 9594, 9753, 9993, 9996, 10102, 11000, 11321, 11371, 13706, 15000, 18183, 18264, 20222, 22289, 22370, 24677, 26264, 27006, 27009, 27960, 30002, 31620, 32786, 37475, 40842, 42510, 42800, 43118, 44337, 44443, 45054, 47891, 49400, 53001 |
| 21 |  | 10.20.202.156 |  | TCP : 427, 902 |
| 22 |  | 10.20.202.157 |  | TCP : 80, 443, 902, 5060, 8000 |
| 23 |  | 10.20.202.158 |  | TCP : 80, 443, 902, 5060, 8000 |
| 24 |  | 10.20.202.181 |  | TCP : 80, 443, 902, 5060, 8000 |
| 25 |  | 10.20.202.183 |  | TCP : 80, 443, 902, 5060, 8000, 8300 |
| 26 |  | 10.20.202.184 |  | TCP : 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8300, 9080 |
| 27 |  | 10.20.202.186 |  | TCP : 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300 |
| 28 |  | 172.23.60.1 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 29 |  | 172.23.60.2 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 30 |  | 172.23.60.3 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 31 |  | 172.23.60.4 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 32 |  | 172.23.60.5 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 33 |  | 172.23.60.10 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 34 |  | 172.23.60.11 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 35 |  | 172.23.60.12 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 36 |  | 172.23.60.13 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 37 |  | 172.23.60.14 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 38 |  | 172.23.60.15 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300 |
| 39 |  | 172.23.60.31 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 40 |  | 172.23.60.32 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300 |
| 41 |  | 172.23.60.33 |  | TCP : 22, 80, 111, 2000, 2020, 2074, 2222, 3205, 3260, 3261, 5060 |
| 42 |  | 172.23.60.34 |  | TCP : 22, 80, 111, 2000, 2020, 2049, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 43 |  | 172.23.60.51 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 44 |  | 172.23.60.52 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 45 |  | 172.23.60.53 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300 |
| 46 |  | 172.23.60.54 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 47 |  | 172.23.60.55 |  | TCP : 22, 80, 427, 443, 902, 2000, 5060, 5989, 8000, 8182, 8300, 9080 |
| 48 |  | 172.23.60.101 |  | TCP : 22, 80, 111, 2000, 2020, 2049, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 49 |  | 172.23.60.102 |  | TCP : 22, 80, 111, 2000, 2020, 2049, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 50 |  | 172.23.60.103 |  | TCP : 22, 80, 111, 2000, 2020, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 51 |  | 172.23.60.104 |  | TCP : 22, 80, 111, 2000, 2020, 2049, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 52 |  | 172.23.60.105 |  | TCP : 22, 80, 111, 2000, 2020, 2049, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 53 |  | 172.23.60.110 |  | TCP : 22, 80, 111, 2000, 2020, 2074, 2222, 3205, 3260, 3261, 5060 |
| 54 |  | 172.23.60.111 |  | TCP : 22, 80, 111, 2000, 2020, 2049, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 55 |  | 172.23.60.112 |  | TCP : 22, 80, 111, 2000, 2020, 2074, 2222, 3205, 3260, 3261, 5060 |
| 56 |  | 172.23.60.113 |  | TCP : 22, 80, 111, 2000, 2020, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 57 |  | 172.23.60.114 |  | TCP : 22, 80, 111, 2000, 2020, 2049, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 58 |  | 172.23.60.115 |  | TCP : 22, 80, 111, 2000, 2020, 2049, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 59 |  | 172.23.60.150 |  | TCP : 22, 80, 88, 389, 443, 514, 636, 1514, 2000, 2012, 2014, 2015, 2020, 5060, 9443 |
| 60 |  | 172.23.60.151 |  | TCP : 22, 80, 111, 2000, 2020, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 61 |  | 172.23.60.152 |  | TCP : 22, 80, 111, 2000, 2020, 2049, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 62 |  | 172.23.60.153 |  | TCP : 22, 80, 111, 2000, 2020, 2049, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 63 |  | 172.23.60.154 |  | TCP : 22, 80, 111, 2000, 2020, 2049, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 64 |  | 172.23.60.155 |  | TCP : 22, 80, 111, 2000, 2020, 2049, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 65 |  | 172.23.60.200 |  | TCP : 22, 80, 111, 2000, 5060 UDP : 111 |
| 66 |  | 172.23.60.201 |  | TCP : 22, 80, 111, 2000, 2020, 2049, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 67 |  | 172.23.60.202 |  | TCP : 22, 80, 111, 2000, 2020, 2049, 2074, 2222, 3205, 3260, 3261, 5060 UDP : 111 |
| 68 |  | 172.23.60.203 |  | TCP : 22, 80, 111, 2000, 2020, 2222, 3205, 3260, 5060 |

## **5.2 Executive summary**

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

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

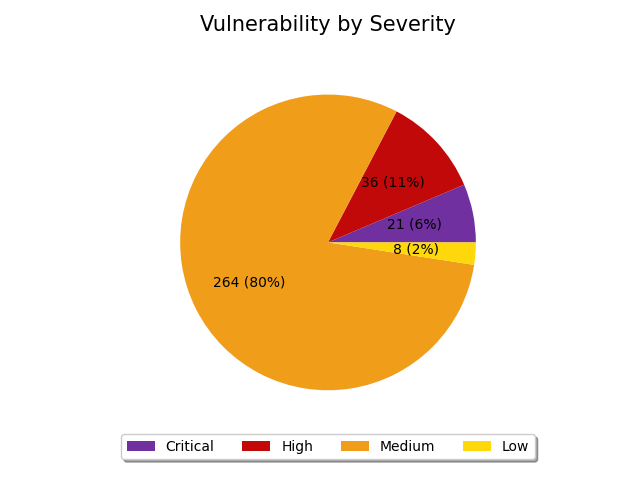


Figure 4: Summary by Severity of Infrastructure Vulnerability Assessment

### **5.2.2 Vulnerability by Target**

| **No.** | **Domain/Server Name** | **IP Address** | **Critical** | **High** | **Medium** | **Low** | **Total** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | - | 10.20.201.101 | 1 | 1 | 4 | 3 | 9 |
| 2 | - | 10.20.202.11 | 0 | 0 | 6 | 0 | 6 |
| 3 | - | 10.20.202.12 | 0 | 0 | 3 | 0 | 3 |
| 4 | - | 10.20.202.13 | 1 | 1 | 5 | 0 | 7 |
| 5 | - | 10.20.202.14 | 0 | 0 | 0 | 0 | 0 |
| 6 | - | 10.20.202.15 | 0 | 0 | 3 | 0 | 3 |
| 7 | - | 10.20.202.16 | 1 | 1 | 10 | 0 | 12 |
| 8 | - | 10.20.202.101 | 0 | 0 | 0 | 0 | 0 |
| 9 | - | 10.20.202.103 | 4 | 15 | 12 | 1 | 32 |
| 10 | - | 10.20.202.104 | 1 | 3 | 5 | 1 | 10 |
| 11 | - | 10.20.202.105 | 5 | 3 | 21 | 1 | 30 |
| 12 | - | 10.20.202.137 | 0 | 1 | 6 | 1 | 8 |
| 13 | - | 10.20.202.138 | 1 | 3 | 6 | 1 | 11 |
| 14 | - | 10.20.202.140 | 0 | 1 | 5 | 0 | 6 |
| 15 | - | 10.20.202.141 | 0 | 0 | 1 | 0 | 1 |
| 16 | - | 10.20.202.151 | 1 | 1 | 8 | 0 | 10 |
| 17 | - | 10.20.202.152 | 1 | 1 | 8 | 0 | 10 |
| 18 | - | 10.20.202.153 | 1 | 1 | 5 | 0 | 7 |
| 19 | - | 10.20.202.154 | 0 | 0 | 0 | 0 | 0 |
| 20 | - | 10.20.202.155 | 0 | 0 | 0 | 0 | 0 |
| 21 | - | 10.20.202.156 | 0 | 0 | 0 | 0 | 0 |
| 22 | - | 10.20.202.157 | 0 | 0 | 0 | 0 | 0 |
| 23 | - | 10.20.202.158 | 0 | 0 | 0 | 0 | 0 |
| 24 | - | 10.20.202.181 | 1 | 1 | 5 | 0 | 7 |
| 25 | - | 10.20.202.183 | 1 | 1 | 5 | 0 | 7 |
| 26 | - | 10.20.202.184 | 1 | 1 | 10 | 0 | 12 |
| 27 | - | 10.20.202.186 | 1 | 1 | 9 | 0 | 11 |
| 28 | - | 172.23.60.1 | 0 | 0 | 4 | 0 | 4 |
| 29 | - | 172.23.60.2 | 0 | 0 | 4 | 0 | 4 |
| 30 | - | 172.23.60.3 | 0 | 0 | 4 | 0 | 4 |
| 31 | - | 172.23.60.4 | 0 | 0 | 4 | 0 | 4 |
| 32 | - | 172.23.60.5 | 0 | 0 | 4 | 0 | 4 |
| 33 | - | 172.23.60.10 | 0 | 0 | 7 | 0 | 7 |
| 34 | - | 172.23.60.11 | 0 | 0 | 5 | 0 | 5 |
| 35 | - | 172.23.60.12 | 0 | 0 | 5 | 0 | 5 |
| 36 | - | 172.23.60.13 | 0 | 0 | 7 | 0 | 7 |
| 37 | - | 172.23.60.14 | 0 | 0 | 5 | 0 | 5 |
| 38 | - | 172.23.60.15 | 0 | 0 | 5 | 0 | 5 |
| 39 | - | 172.23.60.31 | 0 | 0 | 5 | 0 | 5 |
| 40 | - | 172.23.60.32 | 0 | 0 | 5 | 0 | 5 |
| 41 | - | 172.23.60.33 | 0 | 0 | 2 | 0 | 2 |
| 42 | - | 172.23.60.34 | 0 | 0 | 2 | 0 | 2 |
| 43 | - | 172.23.60.51 | 0 | 0 | 3 | 0 | 3 |
| 44 | - | 172.23.60.52 | 0 | 0 | 5 | 0 | 5 |
| 45 | - | 172.23.60.53 | 0 | 0 | 5 | 0 | 5 |
| 46 | - | 172.23.60.54 | 0 | 0 | 3 | 0 | 3 |
| 47 | - | 172.23.60.55 | 0 | 0 | 7 | 0 | 7 |
| 48 | - | 172.23.60.101 | 0 | 0 | 2 | 0 | 2 |
| 49 | - | 172.23.60.102 | 0 | 0 | 2 | 0 | 2 |
| 50 | - | 172.23.60.103 | 0 | 0 | 0 | 0 | 0 |
| 51 | - | 172.23.60.104 | 0 | 0 | 2 | 0 | 2 |
| 52 | - | 172.23.60.105 | 0 | 0 | 2 | 0 | 2 |
| 53 | - | 172.23.60.110 | 0 | 0 | 0 | 0 | 0 |
| 54 | - | 172.23.60.111 | 0 | 0 | 2 | 0 | 2 |
| 55 | - | 172.23.60.112 | 0 | 0 | 2 | 0 | 2 |
| 56 | - | 172.23.60.113 | 0 | 0 | 2 | 0 | 2 |
| 57 | - | 172.23.60.114 | 0 | 0 | 2 | 0 | 2 |
| 58 | - | 172.23.60.115 | 0 | 0 | 2 | 0 | 2 |
| 59 | - | 172.23.60.150 | 0 | 0 | 4 | 0 | 4 |
| 60 | - | 172.23.60.151 | 0 | 0 | 2 | 0 | 2 |
| 61 | - | 172.23.60.152 | 0 | 0 | 2 | 0 | 2 |
| 62 | - | 172.23.60.153 | 0 | 0 | 2 | 0 | 2 |
| 63 | - | 172.23.60.154 | 0 | 0 | 2 | 0 | 2 |
| 64 | - | 172.23.60.155 | 0 | 0 | 2 | 0 | 2 |
| 65 | - | 172.23.60.200 | 0 | 0 | 0 | 0 | 0 |
| 66 | - | 172.23.60.201 | 0 | 0 | 2 | 0 | 2 |
| 67 | - | 172.23.60.202 | 0 | 0 | 2 | 0 | 2 |
| 68 | - | 172.23.60.203 | 0 | 0 | 0 | 0 | 0 |
| **Total** | | | 21 | 36 | 264 | 8 | 329 |

## **5.3 Infrastructure Vulnerability Detail**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 1 | **Finding** | Apache Tomcat 8.5.x 8.5.13 / 9.0.x 9.0.0.M19 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat service running on the remote host is 8.5.x prior to 8.5.13 or  9.0.x prior to 9.0.0.M19. It is therefore affected by multiple  vulnerabilities :  - A flaw exists in the handling of pipelined requests when  send file processing is used that results in the  pipelined request being lost when processing of the  previous request has completed, causing responses to be  sent for the wrong request. An unauthenticated, remote  attacker can exploit this to disclose sensitive  information. (CVE-2017-5647)  - A flaw exists in the handling of HTTP/2 GOAWAY frames  for a connection due to streams associated with the  connection not being properly closed if the connection  was currently waiting for a WINDOW\_UPDATE before  allowing the application to write more data. Each stream  consumes a processing thread in the system. An  unauthenticated, remote attacker can exploit this issue,  via a series of specially crafted HTTP/2 requests, to  consume all available threads, resulting in a denial of  service condition. (CVE-2017-5650)  - A flaw exists in HTTP connectors when processing send  files. If processing completed quickly, it was possible  to add the processor to the processor cache twice, which  allows the same processor to be used for multiple  requests. An unauthenticated, remote attacker can  exploit this to disclose sensitive information from  other sessions or cause unexpected errors.  (CVE-2017-5651) Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.13 / 9.0.0.M19 or later. | | |
| **Remark** | http://www.nessus.org/u?26fc2208 https://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.5.13 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 2 | **Finding** | Apache Tomcat 8.5.0 8.5.32 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 8.5.x prior to 8.5.32. It is, therefore, affected by multiple vulnerabilities. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.32 or later. | | |
| **Remark** | http://www.nessus.org/u?5070a438 http://www.nessus.org/u?d5ab19d6 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 3 | **Finding** | Apache Tomcat 7.0.x 7.0.76 / 8.0.x 8.0.42 / 8.5.x 8.5.12 / 9.0.x 9.0.0.M18 Improper Access Control |
| **Severity** | Critical | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat instance listening on the remote host is 7.0.x prior to 7.0.76, 8.0.x 8.0.42, 8.5.x 8.5.12 or 9.0.x 9.0.0.M18. It is, therefore, affected by the following vulnerability:  - An improper access control vulnerability exists when  calls to application listeners do not use the appropriate  facade object. This allows untrusted applications to  potentially access and modify information associated  with other web applications.  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.76 / 8.0.42 / 8.5.12 / 9.0.0.M18 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.76 http://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.0.42 http://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.5.12 http://www.nessus.org/u?3f871212 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 4 | **Finding** | Apache Tomcat 7.0.x 7.0.100 / 8.5.x 8.5.51 / 9.0.x 9.0.31 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Tomcat installed on the remote host is 7.0.x prior to 7.0.100, 8.x prior to 8.5.51, or 9.0.x prior to 9.0.31. It is, therefore, affected by multiple vulnerabilities.  - An HTTP request smuggling vulnerability exists in Tomcat due to mishandling Transfer-Encoding headers  behind a reverse proxy. An unauthenticated, remote attacker can exploit this, via crafted HTTP requests,  to cause unintended HTTP requests to reach the back-end. (CVE-2019-17569)  - An HTTP request smuggling vulnerability exists in Tomcat due to bad end-of-line (EOL) parsing that allowed  some invalid HTTP headers to be parsed as valid. An unauthenticated, remote attacker can exploit this, via  crafted HTTP requests, to cause unintended HTTP requests to reach the back-end. (CVE-2020-1935)  - An arbitrary file read vulnerability exists in Tomcat's Apache JServ Protocol (AJP) due to an  implementation defect. A remote, unauthenticated attacker could exploit this to access files which, under  normal conditions, would be restricted. If the Tomcat instance supports file uploads, the vulnerability  could also be leveraged to achieve remote code execution. (CVE-2020-1938) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version  number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.100, 8.5.51, 9.0.31 or later. | | |
| **Remark** | https://www.cnvd.org.cn/webinfo/show/5415 http://www.nessus.org/u?8ebe6246 http://www.nessus.org/u?4e287adb http://www.nessus.org/u?cbc3d54e | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 5 | **Finding** | Microsoft SQL Server Unsupported Version Detection (remote check) |
| **Severity** | Critical | **Port** | TCP: 1433, 49185 |
| **Target** | 10.20.202.104(49185), 10.20.202.138(1433) | | |
| **Detail** | According to its self-reported version number, the installation of Microsoft SQL Server on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. | | |
| **Solution** | Upgrade to a version of Microsoft SQL Server that is currently supported. | | |
| **Remark** | http://www.nessus.org/u?d4418a57 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 6 | **Finding** | VMware vCenter Server 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0002) |
| **Severity** | Critical | **Port** | TCP: 443 |
| **Target** | 10.20.202.105(443) | | |
| **Detail** | The version of VMware vCenter Server installed on the remote host is 6.5 prior to 6.5 U3n, 6.7 prior to 6.7 U3l or 7.0 prior to 7.0 U1c. It is, therefore, affected by multiple vulnerabilities, as follows:  - The vSphere Client (HTML5) contains a remote code execution vulnerability in a vCenter Server plugin. A malicious  actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the  underlying operating system that hosts vCenter Server. This affects VMware vCenter Server (7.x before 7.0 U1c, 6.7  before 6.7 U3l and 6.5 before 6.5 U3n) and VMware Cloud Foundation (4.x before 4.2 and 3.x before 3.10.1.2).  (CVE-2021-21972)  - The vSphere Client (HTML5) contains an SSRF (Server Side Request Forgery) vulnerability due to improper validation  of URLs in a vCenter Server plugin. A malicious actor with network access to port 443 may exploit this issue by  sending a POST request to vCenter Server plugin leading to information disclosure. This affects: VMware vCenter  Server (7.x before 7.0 U1c, 6.7 before 6.7 U3l and 6.5 before 6.5 U3n) and VMware Cloud Foundation (4.x before 4.2  and 3.x before 3.10.1.2). (CVE-2021-21973) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version  number. Nessus has also not tested for the presence of a workaround. | | |
| **Solution** | Upgrade to VMware vCenter Server 6.5 U3n, 6.7 U3l, 7.0 U1c or later or apply the workaround mentioned in the advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2021-0002.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 7 | **Finding** | Python Unsupported Version Detection |
| **Severity** | Critical | **Port** | TCP: 6501, 6502 |
| **Target** | 10.20.202.105(6501, 6502) | | |
| **Detail** | The remote host contains one or more unsupported versions of Python. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. | | |
| **Solution** | Upgrade to a version of Python that is currently supported. | | |
| **Remark** | https://www.python.org/downloads/ https://devguide.python.org/devcycle/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 8 | **Finding** | VMware vCenter Server 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0010) |
| **Severity** | Critical | **Port** | TCP: 443 |
| **Target** | 10.20.202.105(443) | | |
| **Detail** | The version of VMware vCenter Server installed on the remote host is 6.5 prior to 6.5 U3p, 6.7 prior to 6.7 U3n or 7.0 prior to 7.0 U2b. It is, therefore, affected by multiple vulnerabilities:  - The vSphere Client (HTML5) contains a remote code execution vulnerability due to lack of input validation in the  Virtual SAN Health Check plug-in which is enabled by default in vCenter Server. A malicious actor with network  access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying  operating system that hosts vCenter Server. (CVE-2021-21985)  - The vSphere Client (HTML5) contains a vulnerability in a vSphere authentication mechanism for the Virtual SAN  Health Check, Site Recovery, vSphere Lifecycle Manager, and VMware Cloud Director Availability plug-ins. A  malicious actor with network access to port 443 on vCenter Server may perform actions allowed by the impacted  plug-ins without authentication. (CVE-2021-21986) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version  number. Nessus has also not tested for the presence of a workaround. | | |
| **Solution** | Upgrade to VMware vCenter Server 6.5 U3p, 6.7 U3n, 7.0 U2b or later or apply the workaround mentioned in the advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2021-0010.html https://blogs.vmware.com/vsphere/2021/05/vmsa-2021-0010.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 9 | **Finding** | VMware vCenter Server 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2021-0027) |
| **Severity** | Critical | **Port** | TCP: 443 |
| **Target** | 10.20.202.105(443) | | |
| **Detail** | The version of VMware vCenter Server installed on the remote host is 6.5 prior to 6.5 U3r or 6.7 prior to 6.7 U3p. It is, therefore, affected by multiple vulnerabilities:  - An arbitrary file read vulnerability exists in the vSphere web client. An unauthenticated, remote attacker  can exploit this, via HTTPS, to gain access to sensitive information. (CVE-2021-21980)  - A server side request forgery vulnerability exists in the vSAN Web Client plug-in. An unauthenticated,  remote attacker can exploit this, via HTTPS, to cause the server to access internal services or access  sites outside of vCenter. (CVE-2021-22049) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version  number. Nessus has also not tested for the presence of a workaround. | | |
| **Solution** | Upgrade to VMware vCenter Server 6.5 U3r, 6.7 U3p, or later. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2021-0027.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 10 | **Finding** | ESXi 6.5 / 6.7 XSS (VMSA-2020-0008) |
| **Severity** | Critical | **Port** | TCP: 443 |
| **Target** | 10.20.202.13(443), 10.20.202.16(443), 10.20.202.151(443), 10.20.202.152(443), 10.20.202.153(443), 10.20.202.181(443), 10.20.202.183(443), 10.20.202.184(443), 10.20.202.186(443) | | |
| **Detail** | The remote VMware ESXi host is version 6.5 or 6.7 and is affected by a cross-site scripting (XSS) vulnerability in virtual machine attributes due to improper validation of user-supplied input before returning it to users. An authenticated, remote attacker with access to modify the system properties of a virtual machine from inside the guest OS can exploit this, by inserting script-related HTML in the system properties and having a user view the system properties from the ESXi Host Client, to execute arbitrary script code in a user's ESXi Host Client session.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2020-0008.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 11 | **Finding** | Unix Operating System Unsupported Version Detection |
| **Severity** | Critical | **Port** | TCP: 0 |
| **Target** | 10.20.201.101(0) | | |
| **Detail** | According to its self-reported version number, the Unix operating system running on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. | | |
| **Solution** | Upgrade to a version of the Unix operating system that is currently supported. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 12 | **Finding** | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| **Severity** | High | **Port** | TCP: 443, 1433, 3389, 49185 |
| **Target** | 10.20.201.101(443), 10.20.202.103(3389), 10.20.202.104(49185), 10.20.202.105(3389), 10.20.202.137(3389), 10.20.202.138(1433), 10.20.202.140(3389) | | |
| **Detail** | The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or  else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network. | | |
| **Solution** | Reconfigure the affected application if possible to avoid use of medium strength ciphers. | | |
| **Remark** | https://www.openssl.org/blog/blog/2016/08/24/sweet32/ https://sweet32.info | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 13 | **Finding** | Apache Tomcat 6.0.16 6.0.50 / 7.0.x 7.0.75 / 8.0.x 8.0.41 / 8.5.x 8.5.9 / 9.0.x 9.0.0.M15 NIO HTTP Connector Information Disclosure |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat service running on the remote host is 6.0.16 prior to 6.0.50, 7.0.x prior to 7.0.75, 8.0.x prior to 8.0.41, 8.5.x prior to 8.5.9, or  9.0.x prior to 9.0.0.M15. It is therefore, affected by an information  disclosure vulnerability in error handling during send file processing  by the NIO HTTP connector, in which an error can cause the current  Processor object to be added to the Processor cache multiple times.  This allows the same Processor to be used for concurrent requests.  An unauthenticated, remote attacker can exploit this issue, via a  shared Processor, to disclose sensitive information, such as session  IDs, response bodies related to another request, etc. Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 6.0.50 / 7.0.75 / 8.0.41 / 8.5.9 /  9.0.0.M15 or later. For the 6.0.x version branch, the vulnerability  was fixed in 6.0.49; however, that release candidate was not approved,  and 6.0.50 is still pending release. | | |
| **Remark** | http://www.nessus.org/u?3a06fd01 https://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.5.9 http://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.0.41 http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.75 http://tomcat.apache.org/security-6.html#Fixed\_in\_Apache\_Tomcat\_6.0.50 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 14 | **Finding** | Apache Tomcat 8.5.7 8.5.11 nextRequest Information Disclosure |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 8.5.7 or later but prior to 8.5.11. It is, therefore, affected by an information disclosure vulnerability in the nextRequest() function in Http11InputBuffer.java due to improper limits of a ByteBuffer being set. An unauthenticated, remote attacker can exploit this to disclose ByteBuffer data associated with a different request. Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.11 or later. Note that the vulnerability was also fixed in version 8.5.10; however, this version was never publicly released. | | |
| **Remark** | http://www.nessus.org/u?09e0bc40 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 15 | **Finding** | Apache Tomcat 7.0.x 7.0.78 / 8.0.x 8.0.44 / 8.5.x 8.5.15 / 9.0.x 9.0.0.M21 Remote Error Page Manipulation |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat service running on the remote host is 7.0.x prior to 7.0.78, 8.0.x prior to 8.0.44, 8.5.x prior to 8.5.15, or 9.0.x prior to 9.0.0.M21. It is, therefore, affected by an implementation flaw in the error  page reporting mechanism in which it does not conform to the Java  Servlet Specification that requires static error pages to be processed  as an HTTP GET request nothwithstanding the HTTP request method that  was originally used when the error occurred. Depending on the original  request and the configuration of the Default Servlet, an  unauthenticated, remote attacker can exploit this issue to replace or  remove custom error pages. Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.78 / 8.0.44 / 8.5.15 / 9.0.0.M21 or later. | | |
| **Remark** | http://tomcat.apache.org/security-7.html#Fixed\_in\_Apache\_Tomcat\_7.0.78 http://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.0.44 http://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.5.15 http://www.nessus.org/u?a774a43b | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 16 | **Finding** | Apache Tomcat 8.5.x 8.5.16 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 8.5.x prior to 8.5.16. It is, therefore, affected by multiple vulnerabilities :  - A flaw exists in the CORS filter because the HTTP Vary header was  not properly added. This allows a remote attacker to conduct  client-side and server-side cache poisoning attacks.  (CVE-2017-7674)  - A flaw exists in the HTTP/2 implementation that bypasses a number  of security checks that prevented directory traversal attacks. A  remote attacker can exploit this to bypass security constraints.  (CVE-2017-7675) Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.16 or later. | | |
| **Remark** | http://www.nessus.org/u?1f8717dc | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 17 | **Finding** | Apache Tomcat 7.0.x 7.0.82 / 8.5.x 8.5.23 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 7.0.x prior to 7.0.82 or 8.5.x prior to 8.5.23. It is, therefore, affected by an unspecified vulnerability when running with HTTP PUTs enabled (e.g. via setting the readonly initialization parameter of the Default to false) that makes it possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server. Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.82 / 8.5.23 or later. | | |
| **Remark** | http://www.nessus.org/u?4f047e41 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 18 | **Finding** | Apache Tomcat 8.0.x 8.0.52 / 8.5.x 8.5.31 / 9.0.x 9.0.8 Denial of Service |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat instance listening on the remote host is 8.0.x 8.0.52,  8.5.x 8.5.31 or 9.0.x 9.0.8. It is, therefore, affected  by the following vulnerability:  - A denial of service (DoS) vulnerability exists in   Tomcat due to improper overflow handling in the UTF-8  decoder. An unauthenticated, remote attacker can exploit   this issue to cause an infinite loop in the decoder,  leading to a denial of service condition. Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.0.52 / 8.5.31 / 9.0.8 or later. | | |
| **Remark** | http://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.0.52 http://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.5.31 http://tomcat.apache.org/security-9.html#Fixed\_in\_Apache\_Tomcat\_9.0.8 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 19 | **Finding** | Apache Tomcat 8.5.0 8.5.41 DoS |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.41. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_8.5.41\_security-8 advisory.  - The fix for CVE-2019-0199 was incomplete and did not  address HTTP/2 connection window exhaustion on write. By  not sending WINDOW\_UPDATE messages for the connection  window (stream 0) clients were able to cause server-side  threads to block eventually leading to thread exhaustion  and a DoS. (CVE-2019-10072) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.41 or later. | | |
| **Remark** | https://github.com/apache/tomcat/commit/0bcd69c https://github.com/apache/tomcat/commit/8d14c6f https://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.5.41 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 20 | **Finding** | Apache Tomcat 8.5.0 8.5.49 Privilege Escalation |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.49. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_8.5.49\_security-8 advisory.  - When Apache Tomcat is configured with the JMX Remote   Lifecycle Listener, a local attacker without access to   the Tomcat process or configuration files is able to   manipulate the RMI registry to perform a man-in-the-middle   attack to capture user names and passwords used to access   the JMX interface. The attacker can then use these   credentials to access the JMX interface and gain complete   control over the Tomcat instance. (CVE-2019-12418) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.49 or later. | | |
| **Remark** | https://github.com/apache/tomcat/commit/a91d7db http://www.nessus.org/u?ed6582f2 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 21 | **Finding** | Apache Tomcat 8.5.0 8.5.50 Privilege Escalation Vulnerability |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.50. It is, therefore, affected by a privilege escalation vulnerability as referenced in the 'Fixed in Apache Tomcat 8.5.50' advisory.  - When using FORM authentication there was a narrow window where an attacker could perform a session  fixation attack. The window was considered too narrow for an exploit to be practical but, erring on the  side of caution, this issue has been treated as a security vulnerability. (CVE-2019-17563) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.50 or later. | | |
| **Remark** | https://github.com/apache/tomcat/commit/e19a202 http://www.nessus.org/u?e0b173ef | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 22 | **Finding** | Apache Tomcat 8.5.x 8.5.55 Remote Code Execution |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.x prior to 8.5.55. It is, therefore, affected by a  remote code execution vulnerability as referenced in the fixed\_in\_apache\_tomcat\_8.5.55\_security-8 advisory.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version  number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.55 or later. | | |
| **Remark** | http://www.nessus.org/u?9502c510 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 23 | **Finding** | Apache Tomcat 8.5.0 8.5.56 DoS |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.56. It is, therefore, affected by a denial of service vulnerability as referenced in the fixed\_in\_apache\_tomcat\_8.5.56\_security-8 advisory. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.56 or later. | | |
| **Remark** | http://www.nessus.org/u?9a501720 http://www.nessus.org/u?0ff2bf8c | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 24 | **Finding** | Apache Tomcat 8.5.0 8.5.57 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Tomcat installed on the remote host is 8.5.x prior to 8.5.57. It is, therefore, affected by multiple vulnerabilities as referenced in the Fixed in Apache Tomcat 8.5.57 security advisory.  - The payload length in a WebSocket frame was not correctly validated. Invalid payload lengths could trigger  an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service (DoS).  (CVE-2020-13935)  - An h2c direct connection did not release the HTTP/1.1 processor after the upgrade to HTTP/2. If a  sufficient number of such requests were made, an OutOfMemoryException could occur leading to a denial of  service (DoS). (CVE-2020-13934) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.57 or later. | | |
| **Remark** | http://www.nessus.org/u?cd59de72 http://www.nessus.org/u?7358785a http://www.nessus.org/u?78f0e4ba | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 25 | **Finding** | Apache Tomcat 8.5.x 8.5.60 Information Disclosure |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.60. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed\_in\_apache\_tomcat\_8.5.60\_security-8 advisory.  - When serving resources from a network location using the NTFS file system, Apache Tomcat versions  10.0.0-M1 to 10.0.0-M9, 9.0.0.M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP  source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE API  File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API  (FindFirstFileW) in some circumstances. (CVE-2021-24122)  - While investigating bug 64830 it was discovered that Apache Tomcat 10.0.0-M1 to 10.0.0-M9, 9.0.0-M1 to  9.0.39 and 8.5.0 to 8.5.59 could re-use an HTTP request header value from the previous stream received on  an HTTP/2 connection for the request associated with the subsequent stream. While this would most likely  lead to an error and the closure of the HTTP/2 connection, it is possible that information could leak  between requests. (CVE-2020-17527) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.60 or later. | | |
| **Remark** | http://www.nessus.org/u?05c4b1e2 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 26 | **Finding** | Apache Tomcat 8.5.0 8.5.63 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.63. It is, therefore, affected by multiple vulnerabilities as referenced in the vendor advisory.  - When responding to new h2c connection requests, Apache Tomcat versions 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41   and 8.5.0 to 8.5.61 could duplicate request headers and a limited amount of request body from one request to   another meaning user A and user B could both see the results of user A's request. (CVE-2021-25122)  - When using Apache Tomcat 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41, 8.5.0 to 8.5.61 or 7.0.0. to 7.0.107 with a   configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to   CVE-2020-9494. Note that both the previously published prerequisites for CVE-2020-9484 and the previously   published mitigations for CVE-2020-9484 also apply to this issue. (CVE-2021-25329) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.63 or later. | | |
| **Remark** | http://www.nessus.org/u?b6278e74 http://www.nessus.org/u?0be223a3 http://www.nessus.org/u?15b6baad | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 27 | **Finding** | SSL Version 2 and 3 Protocol Detection |
| **Severity** | High | **Port** | TCP: 1433, 49185 |
| **Target** | 10.20.202.104(49185), 10.20.202.138(1433) | | |
| **Detail** | The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:  - An insecure padding scheme with CBC ciphers.  - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients. Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely. NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'. | | |
| **Solution** | Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead. | | |
| **Remark** | https://www.schneier.com/academic/paperfiles/paper-ssl.pdf http://www.nessus.org/u?b06c7e95 http://www.nessus.org/u?247c4540 https://www.openssl.org/~bodo/ssl-poodle.pdf http://www.nessus.org/u?5d15ba70 https://www.imperialviolet.org/2014/10/14/poodle.html https://tools.ietf.org/html/rfc7507 https://tools.ietf.org/html/rfc7568 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 28 | **Finding** | SSL Certificate Signed Using Weak Hashing Algorithm |
| **Severity** | High | **Port** | TCP: 1433, 49185 |
| **Target** | 10.20.202.104(49185), 10.20.202.138(1433) | | |
| **Detail** | The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm. Note that certificates in the chain that are contained in the Nessus CA database (known\_CA.inc) have been ignored. | | |
| **Solution** | Contact the Certificate Authority to have the SSL certificate reissued. | | |
| **Remark** | https://tools.ietf.org/html/rfc3279 http://www.nessus.org/u?9bb87bf2 http://www.nessus.org/u?e120eea1 http://www.nessus.org/u?5d894816 http://www.nessus.org/u?51db68aa http://www.nessus.org/u?9dc7bfba | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 29 | **Finding** | VMware vCenter Server 6.5 / 6.7 Session Hijack (VMSA-2020-0023) |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.105(443) | | |
| **Detail** | The version of VMware vCenter Server installed on the remote host is 6.5 prior to 6.5u3k or 6.7 prior to 6.7u3. It is, therefore, affected by a session hijack vulnerability in the vCenter Server Appliance. Management Interface update function due to a lack of certificate validation. A malicious actor with network positioning between vCenter Server and an update repository may be able to perform a session hijack when the vCenter Server Appliance Management Interface is used to download vCenter updates. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version  number. | | |
| **Solution** | Upgrade to VMware vCenter Server 6.5u3k, 6.7u3 or later. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2020-0023.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 30 | **Finding** | VMware vCenter Server 6.5 U3q Multiple Vulnerabilities (VMSA-2021-0020) |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.105(443) | | |
| **Detail** | The version of VMware vCenter Server installed on the remote host is 6.5 prior to 6.5 U3q. It is, therefore, affected  by multiple vulnerabilities:  - A privilege escalation vulnerability exists in vCenter Server due to the way it handles session tokens.   An authenticated, local attacker can exploit this to gain unauthorized access to the system.   (CVE-2021-21991, CVE-2021-22015)  - An rhttproxy bypass vulnerability exists in vCenter Server due to improper implementation of URI  normalization. An unauthenticated, remote attacker can exploit this to gain access to internal  endpoints. (CVE-2021-22017) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version  number. Nessus has also not tested for the presence of a workaround. | | |
| **Solution** | Upgrade to VMware vCenter Server 6.5 U3q or later or apply the workaround mentioned in the advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2021-0020.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 31 | **Finding** | ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026) |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.20.202.13(443), 10.20.202.16(443), 10.20.202.151(443), 10.20.202.152(443), 10.20.202.153(443), 10.20.202.181(443), 10.20.202.183(443), 10.20.202.184(443), 10.20.202.186(443) | | |
| **Detail** | According to its self-reported version number, the remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by multiple vulnerabilities.    - A use-after-free error exists in the XHCI USB controller. An unauthenticated, local attacker with local  administrative privileges on a virtual machine can exploit this, to execute code as the virtual machine's  VMX process running on the host. (CVE-2020-4004)   - A privilege escalation vulnerability exists in ESXi due to how certain system calls are managed. An  authenticated, local attacker with privileges within the VPM process can exploit this, when chained with  CVE-2020-4004, to obtain escalated privileges. (CVE-2020-4005)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2020-0026.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 32 | **Finding** | Apache Tomcat Default Files |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself. | | |
| **Solution** | Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to  replace or modify the default error page. | | |
| **Remark** | http://www.nessus.org/u?4cb3b4dd https://www.owasp.org/index.php/Securing\_tomcat | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 33 | **Finding** | SSL Certificate Cannot Be Trusted |
| **Severity** | Medium | **Port** | TCP: 443, 636, 1433, 1514, 2074, 3389, 5989, 6501, 6502, 8182, 9080, 9443, 49185 |
| **Target** | 10.20.201.101(443), 10.20.202.11(443, 9080), 10.20.202.12(9080), 10.20.202.13(9080), 10.20.202.15(9080), 10.20.202.16(443, 8182, 9080), 10.20.202.103(443, 3389), 10.20.202.104(49185), 10.20.202.105(443, 1514, 3389, 6501, 6502, 9443), 10.20.202.137(3389), 10.20.202.138(1433), 10.20.202.140(3389), 10.20.202.151(443, 9080), 10.20.202.152(443, 9080), 10.20.202.153(443), 10.20.202.181(443), 10.20.202.183(443), 10.20.202.184(443, 5989, 9080), 10.20.202.186(443, 5989, 8182), 172.23.60.1(5989, 8182), 172.23.60.2(5989, 8182), 172.23.60.3(5989, 8182), 172.23.60.4(5989, 8182), 172.23.60.5(5989, 8182), 172.23.60.10(443, 5989, 8182, 9080), 172.23.60.11(443, 5989, 8182), 172.23.60.12(443, 5989, 8182), 172.23.60.13(443, 5989, 8182, 9080), 172.23.60.14(443, 8182, 9080), 172.23.60.15(443, 5989, 8182), 172.23.60.31(443, 5989, 8182), 172.23.60.32(443, 5989, 8182), 172.23.60.33(2074), 172.23.60.34(2074), 172.23.60.51(443, 5989), 172.23.60.52(443, 5989, 8182), 172.23.60.53(443, 5989, 8182), 172.23.60.54(443, 9080), 172.23.60.55(443, 5989, 8182, 9080), 172.23.60.101(2074), 172.23.60.102(2074), 172.23.60.104(2074), 172.23.60.105(2074), 172.23.60.111(2074), 172.23.60.112(2074), 172.23.60.113(2074), 172.23.60.114(2074), 172.23.60.115(2074), 172.23.60.150(443, 636, 1514, 9443), 172.23.60.151(2074), 172.23.60.152(2074), 172.23.60.153(2074), 172.23.60.154(2074), 172.23.60.155(2074), 172.23.60.201(2074), 172.23.60.202(2074) | | |
| **Detail** | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the  server might not be descended from a known public  certificate authority. This can occur either when the  top of the chain is an unrecognized, self-signed  certificate, or when intermediate certificates are  missing that would connect the top of the certificate  chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate  that is not valid at the time of the scan. This can  occur either when the scan occurs before one of the  certificate's 'notBefore' dates, or after one of the  certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature  that either didn't match the certificate's information  or could not be verified. Bad signatures can be fixed by  getting the certificate with the bad signature to be  re-signed by its issuer. Signatures that could not be  verified are the result of the certificate's issuer  using a signing algorithm that Nessus either does not  support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and  identity of the web server. This could make it easier to carry out  man-in-the-middle attacks against the remote host. | | |
| **Solution** | Purchase or generate a proper SSL certificate for this service. | | |
| **Remark** | https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 34 | **Finding** | SSL Self-Signed Certificate |
| **Severity** | Medium | **Port** | TCP: 443, 1433, 2074, 3389, 5989, 8182, 9080, 49185 |
| **Target** | 10.20.201.101(443), 10.20.202.11(443, 9080), 10.20.202.12(9080), 10.20.202.13(9080), 10.20.202.15(9080), 10.20.202.16(443, 9080), 10.20.202.103(3389), 10.20.202.104(49185), 10.20.202.105(3389), 10.20.202.137(3389), 10.20.202.138(1433), 10.20.202.140(3389), 10.20.202.151(443, 9080), 10.20.202.152(443, 9080), 10.20.202.153(443), 10.20.202.181(443), 10.20.202.183(443), 10.20.202.184(443, 9080), 10.20.202.186(443), 172.23.60.1(5989, 8182), 172.23.60.2(5989, 8182), 172.23.60.3(5989, 8182), 172.23.60.4(5989, 8182), 172.23.60.5(5989, 8182), 172.23.60.10(5989, 8182, 9080), 172.23.60.11(5989, 8182), 172.23.60.12(5989, 8182), 172.23.60.13(5989, 8182, 9080), 172.23.60.14(8182, 9080), 172.23.60.15(5989, 8182), 172.23.60.31(5989, 8182), 172.23.60.32(5989, 8182), 172.23.60.33(2074), 172.23.60.34(2074), 172.23.60.51(5989), 172.23.60.52(5989, 8182), 172.23.60.53(5989, 8182), 172.23.60.54(9080), 172.23.60.55(5989, 8182, 9080), 172.23.60.101(2074), 172.23.60.102(2074), 172.23.60.104(2074), 172.23.60.105(2074), 172.23.60.111(2074), 172.23.60.112(2074), 172.23.60.113(2074), 172.23.60.114(2074), 172.23.60.115(2074), 172.23.60.151(2074), 172.23.60.152(2074), 172.23.60.153(2074), 172.23.60.154(2074), 172.23.60.155(2074), 172.23.60.201(2074), 172.23.60.202(2074) | | |
| **Detail** | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. | | |
| **Solution** | Purchase or generate a proper SSL certificate for this service. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 35 | **Finding** | SMB Signing not required |
| **Severity** | Medium | **Port** | TCP: 445 |
| **Target** | 10.20.202.103(445), 10.20.202.105(445), 10.20.202.137(445), 10.20.202.138(445), 10.20.202.140(445), 10.20.202.141(445) | | |
| **Detail** | Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. | | |
| **Solution** | Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. | | |
| **Remark** | http://www.nessus.org/u?df39b8b3 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html http://www.nessus.org/u?a3cac4ea | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 36 | **Finding** | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
| **Severity** | Medium | **Port** | TCP: 443, 1433, 3389, 49185 |
| **Target** | 10.20.201.101(443), 10.20.202.103(3389), 10.20.202.104(49185), 10.20.202.105(3389), 10.20.202.137(3389), 10.20.202.138(1433), 10.20.202.140(3389) | | |
| **Detail** | The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext. | | |
| **Solution** | Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support. | | |
| **Remark** | https://www.rc4nomore.com/ http://www.nessus.org/u?ac7327a0 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ https://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 37 | **Finding** | TLS Version 1.0 Protocol Detection |
| **Severity** | Medium | **Port** | TCP: 443, 1433, 3389, 5989, 6501, 6502, 8182, 9080, 9443, 49185 |
| **Target** | 10.20.201.101(443), 10.20.202.11(443, 9080), 10.20.202.12(9080), 10.20.202.13(9080), 10.20.202.15(9080), 10.20.202.16(443, 8182, 9080), 10.20.202.103(443, 3389), 10.20.202.104(49185), 10.20.202.105(443, 3389, 6501, 6502, 9443), 10.20.202.137(3389), 10.20.202.138(1433), 10.20.202.140(3389), 10.20.202.151(443, 9080), 10.20.202.152(443, 9080), 10.20.202.153(443), 10.20.202.181(443), 10.20.202.183(443), 10.20.202.184(443, 5989, 9080), 10.20.202.186(443, 5989, 8182) | | |
| **Detail** | The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.  As of March 31, 2020, Endpoints that aren’t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.  PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits. | | |
| **Solution** | Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0. | | |
| **Remark** | https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 38 | **Finding** | Apache Tomcat 8.5.x 8.5.34 Open Redirect Weakness |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 8.5.x prior to 8.5.34. It is, therefore, affected by a open redirect  vulnerability. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.34 or later. | | |
| **Remark** | http://www.nessus.org/u?1bddf0bb | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 39 | **Finding** | Apache Tomcat 8.5.x 8.5.58 / 9.0.x 9.0.38 HTTP/2 Request Mix-Up |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Tomcat installed on the remote host is 8.5.x prior to 8.5.58 or 9.0.x prior to 9.0.38. It is, therefore, affected by a vulnerability. If an HTTP/2 client exceeds the agreed maximum number of concurrent streams for a connection (in violation of the HTTP/2 protocol), it is possible that a subsequent request made on that connection could contain HTTP headers - including HTTP/2 pseudo headers - from a previous request rather than the intended headers. This can lead to users seeing responses for unexpected resources. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.58, 9.0.38 or later. | | |
| **Remark** | http://www.nessus.org/u?0656cf04 http://www.nessus.org/u?771617a1 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 40 | **Finding** | Apache Tomcat 7.0.x = 7.0.108 / 8.5.x = 8.5.65 / 9.0.x = 9.0.45 / 10.0.x = 10.0.5 vulnerability |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Tomcat installed on the remote host is 7.0.x = 7.0.108 / 8.5.x = 8.5.65 / 9.0.x = 9.0.45 / 10.0.x =  10.0.5. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_10.0.6\_security-10  advisory.  - Queries made by the JNDI Realm did not always correctly escape parameters. Parameter values could be  sourced from user provided data (eg user names) as well as configuration data provided by an  administrator. In limited circumstances it was possible for users to authenticate using variations of  their user name and/or to bypass some of the protection provided by the LockOut Realm. (CVE-2021-30640) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.109, 8.5.66, 9.0.46, 10.0.6 or later. | | |
| **Remark** | http://www.nessus.org/u?d3fb2d8e http://www.nessus.org/u?0fb6f5ab http://www.nessus.org/u?0d761c19 http://www.nessus.org/u?ddfa2b5e http://www.nessus.org/u?95156892 http://www.nessus.org/u?ed08487c http://www.nessus.org/u?806274b5 http://www.nessus.org/u?f104a57d https://bz.apache.org/bugzilla/show\_bug.cgi?id=65224 http://www.nessus.org/u?837a9443 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 41 | **Finding** | Apache Tomcat 8.5.0 8.5.68 vulnerability |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.68. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_8.5.68\_security-8 advisory.  - Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP  transfer-encoding request header in some circumstances leading to the possibility to request smuggling  when used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if  the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding;  and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.  (CVE-2021-33037) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.68 or later. | | |
| **Remark** | http://www.nessus.org/u?ca148f18 http://www.nessus.org/u?9e0e6b06 http://www.nessus.org/u?bea8fba1 http://www.nessus.org/u?836aea5f | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 42 | **Finding** | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |
| **Severity** | Medium | **Port** | TCP: 1433, 49185 |
| **Target** | 10.20.202.104(49185), 10.20.202.138(1433) | | |
| **Detail** | The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections. As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service. The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism. This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability. | | |
| **Solution** | Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled. | | |
| **Remark** | https://www.imperialviolet.org/2014/10/14/poodle.html https://www.openssl.org/~bodo/ssl-poodle.pdf https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 43 | **Finding** | Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness |
| **Severity** | Medium | **Port** | TCP: 3389 |
| **Target** | 10.20.202.105(3389), 10.20.202.137(3389) | | |
| **Detail** | The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP  client makes no effort to validate the identity of the server when  setting up encryption. An attacker with the ability to intercept  traffic from the RDP server can establish encryption with the client  and server without being detected. A MiTM attack of this nature would  allow the attacker to obtain any sensitive information transmitted,  including authentication credentials. This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack. | | |
| **Solution** | - Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote  Desktop with Network Level Authentication' setting if it is available. | | |
| **Remark** | http://www.nessus.org/u?8033da0d http://technet.microsoft.com/en-us/library/cc782610.aspx | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 44 | **Finding** | Terminal Services Doesn't Use Network Level Authentication (NLA) Only |
| **Severity** | Medium | **Port** | TCP: 3389 |
| **Target** | 10.20.202.105(3389) | | |
| **Detail** | The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication,  NLA also helps protect the remote computer from malicious users and  software by completing user authentication before a full RDP  connection is established. | | |
| **Solution** | Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows. | | |
| **Remark** | https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11) http://www.nessus.org/u?e2628096 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 45 | **Finding** | VMware vCenter Server 5.5.x 5.5U3g / 6.0.x 6.0U3d / 6.5.x 6.5U1e Hypervisor-Assisted Guest Remediation (VMSA-2018-0004) (Spectre) |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 10.20.202.105(443) | | |
| **Detail** | The version of VMware vCenter Server installed on the remote host is 5.5.x prior to 5.5U3g, 6.0.x prior to 6.0U3d, or 6.5.x prior to 6.5U1e. It is, therefore, missing security updates that add hypervisor-assisted guest remediation for a speculative execution vulnerability (CVE-2017-5715). | | |
| **Solution** | Upgrade to VMware vCenter Server version 5.5.U3g (5.5.0 build-7460778) / 6.0U3d (6.0.0 build-7464194) / 6.5U1e (6.5.0 build-7515524) or later. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2018-0004.html https://kb.vmware.com/s/article/52085 https://spectreattack.com/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 46 | **Finding** | VMware vCenter Server 6.5.x 6.5u1f Multiple Vulnerabilities (VMSA-2018-0007) (Spectre-1) (Meltdown) |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 10.20.202.105(443) | | |
| **Detail** | The version of VMware vCenter Server installed on the remote host is 6.5.x prior to 6.5u1f. It is, therefore, affected by multiple vulnerabilities. See advisory for details. | | |
| **Solution** | Upgrade to VMware vCenter Server version 6.5u1f (6.5.0 build-7801515) or later. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2018-0007.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 47 | **Finding** | VMware vCenter Server 5.5.x / 6.0.x / 6.5.x / 6.7.x Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020) |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 10.20.202.105(443) | | |
| **Detail** | The version of VMware vCenter Server installed on the remote host is 5.5.x prior to 5.5u3j, 6.0.x prior to 6.0u3h, 6.5.x prior to 6.5u2c, or 6.7.x prior to 6.7.0d. It is, therefore, affected by a speculative execution side channel attack known as L1 Terminal Fault (L1TF). An attacker who successfully exploited L1TF may be able to read privileged data across trust boundaries. | | |
| **Solution** | Upgrade to the version, or later, referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2018-0020.html https://foreshadowattack.eu/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 48 | **Finding** | VMware vCenter Server 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0013) |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 10.20.202.105(443) | | |
| **Detail** | The version of VMware vCenter Server installed on the remote host is 6.0 prior to U3j, 6.5 prior to U3, or 6.7 prior to U3, and is, therefore, affected by the following vulnerabilities:  - An information disclosure vulnerability caused by  insufficient session expiration. This allows an  attacker with physical access or the ability to mimic  a websocket connection to a user's browser to control a  VM console after the user's session has expired or they  have logged out. (CVE-2019-5531)  - An information disclosure vulnerability caused by  plain-text logging of virtual machine credentials  through OVF. This allows an attacker with access to the  log files which contain the vCenter OVF-properties of a  virtual machine deployed from an OVF to view the  credentials used to deploy the OVF, which typically  belong to the root account of the virtual machine.  (CVE-2019-5532)  - An information disclosure vulnerability in virtual  machines deployed from an OVF which could expose login  information via the virtual machine's vAppConfig  properties. An attacker with access to query the  vAppConfig properties of a virtual machine deployed  from an OVF can view the credentials used to deploy the  OVC, which typically belong to the root account of the  virtual machine. (CVE-2019-5534)   Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to VMware vCenter Server 6.0 U3j, 6.5 U3, or 6.7 U3 or later. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2019-0013.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 49 | **Finding** | VMware vCenter Server 6.5 / 6.7 / 7.0 DoS (VMSA-2020-0018) |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 10.20.202.105(443) | | |
| **Detail** | The version of VMware vCenter Server installed on the remote host is 6.5 prior to 6.5u3k, 6.7 prior to 6.7u3j or 7.0 prior to 7.0.0b. It is, therefore, affected by a denial of service vulnerability (DoS) in the authentication service. An unauthenticated, remote attacker can exploit this issue to exhaust memory resources resulting in a degradation of performance condition while the attack is sustained.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version  number. | | |
| **Solution** | Upgrade to VMware vCenter Server 6.5u3k, 6.7u3j, 7.0.0b or later. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2020-0018.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 50 | **Finding** | ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0005) (Remote Check) |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 10.20.202.13(443), 10.20.202.16(443), 10.20.202.151(443), 10.20.202.152(443), 10.20.202.153(443), 10.20.202.181(443), 10.20.202.183(443), 10.20.202.184(443), 10.20.202.186(443) | | |
| **Detail** | The remote VMware ESXi host is version 6.0, 6.5, or 6.7 and is missing a security patch. It is, therefore, vulnerable to multiple vulnerabilities, including:   - An out-of-bounds read/write vulnerability and a Time-of-check  Time-of-use (TOCTOU) vulnerability in the virtual USB 1.1 UHCI  (Universal Host Controller Interface). Exploitation of these  issues requires an attacker to have access to a virtual machine  with a virtual USB controller present. These issues may allow a  guest to execute code on the host. (CVE-2019-5518, CVE-2019-5519) | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2019-0005.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 51 | **Finding** | ESXi 6.5 / 6.7 / 7.0 DoS (VMSA-2020-0018) |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 10.20.202.13(443), 10.20.202.16(443), 10.20.202.151(443), 10.20.202.152(443), 10.20.202.153(443), 10.20.202.181(443), 10.20.202.183(443), 10.20.202.184(443), 10.20.202.186(443) | | |
| **Detail** | The remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by a denial of service (DoS) vulnerability in the authentication service. An unauthenticated, remote attacker can exploit this issue to exhaust memory resources  resulting in a degradation of performance condition while the attack is sustained.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2020-0018.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 52 | **Finding** | Apache Tomcat 8.5.x 8.5.28 Security Constraint Weakness |
| **Severity** | Low | **Port** | TCP: 443 |
| **Target** | 10.20.202.103(443) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 8.5.x prior to 8.5.28. It is, therefore, affected by a security constraints flaw which could expose resources to unauthorized users. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.28 or later. | | |
| **Remark** | http://www.nessus.org/u?bebc5536 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 53 | **Finding** | SSL Certificate Chain Contains RSA Keys Less Than 2048 bits |
| **Severity** | Low | **Port** | TCP: 1433, 49185 |
| **Target** | 10.20.202.104(49185), 10.20.202.138(1433) | | |
| **Detail** | At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits. Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014. Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt. | | |
| **Solution** | Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate. | | |
| **Remark** | https://www.cabforum.org/wp-content/uploads/Baseline\_Requirements\_V1.pdf | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 54 | **Finding** | Terminal Services Encryption Level is not FIPS-140 Compliant |
| **Severity** | Low | **Port** | TCP: 3389 |
| **Target** | 10.20.202.105(3389), 10.20.202.137(3389) | | |
| **Detail** | The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant. | | |
| **Solution** | Change RDP encryption level to :  4. FIPS Compliant | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 55 | **Finding** | SSH Server CBC Mode Ciphers Enabled |
| **Severity** | Low | **Port** | TCP: 22 |
| **Target** | 10.20.201.101(22) | | |
| **Detail** | The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.  Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions. | | |
| **Solution** | Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 56 | **Finding** | SSH Weak MAC Algorithms Enabled |
| **Severity** | Low | **Port** | TCP: 22 |
| **Target** | 10.20.201.101(22) | | |
| **Detail** | The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak. Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions. | | |
| **Solution** | Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 57 | **Finding** | SSH Weak Key Exchange Algorithms Enabled |
| **Severity** | Low | **Port** | TCP: 22 |
| **Target** | 10.20.201.101(22) | | |
| **Detail** | The remote SSH server is configured to allow key exchange algorithms which are considered weak. This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:  diffie-hellman-group-exchange-sha1  diffie-hellman-group1-sha1  gss-gex-sha1-\*  gss-group1-sha1-\*  gss-group14-sha1-\*  rsa1024-sha1 Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions. | | |
| **Solution** | Contact the vendor or consult product documentation to disable the weak algorithms. | | |
| **Remark** | http://www.nessus.org/u?b02d91cd https://datatracker.ietf.org/doc/html/rfc8732 | | |



# Web Application Vulnerability Assessment

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

**Testing date:** March 30, 2021

**Tester IP Address:** 203.150.79.252

Diagram

Description automatically generated

Figure 5: Vulnerability Assessment from Public Access

## **6.1 Target Information**

| **No.** | **Domain / Server Name** | **IP Address** | **OS/Model** | **Port** |
| --- | --- | --- | --- | --- |
| 1 | https://example.com | 123.123.123.123 | Ubuntu 20 | TCP 22, 53, 80, 113, 123, 443, 2000, 4118, 4119, 4120, 4121, 4122, 4444, 5000, 5060, 8008, 8082 |

## **6.2 Executive summary**

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

### **6.2.1 Summary Vulnerability by Severity**

Figure 6: Summary by Severity of Web Application Vulnerability Assessment

### **6.2.2 Vulnerability by Target**

| **No.** | **Domain/Server Name** | **IP Address** | **Critical** | **High** | **Medium** | **Low** | **Total** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | https://example.com | 123.123.123.123 | 0 | 0 | 1 | 3 | 4 |
| **Total** | | | **0** | **0** | **1** | **3** | **4** |

## **6.3 Web Application Vulnerability Detail**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 1 | **Finding** | Clickjacking: X-Frame-Options header |
| **Severity** | **Low** | **Port** | TCP 443 |
| **Target** | https://example.com/  https://example.com/sitemap.xml  https://example.com/sitemap.xml.gz  https://example.com/login  https://example.com/backend/  https://example.com/backend/api/v1/  https://example.com/backend/api/  https://example.com/backend.bak  https://example.com/backend.7z  https://example.com/backend.cfg  https://example.com/backend.csv  https://example.com/backend.dump  https://example.com/backend.ini  https://example.com/backend.jar  https://example.com/backend.old  https://example.com/backend.ost  https://example.com/backend.pst  https://example.com/backend.sh  https://example.com/backend.sln  https://example.com/backend.tar  https://example.com/backend.war | | |
| **Detail** | Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information, or taking control of their computer while clicking on seemingly innocuous web pages.  The server did not return an X-Frame-Options header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites. | | |
| **Impact** | The impact depends on the affected web application. | | |
| **Solution** | Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 2 | **Finding** | HTTP Strict Transport Security (HSTS) not implemented |
| **Severity** | **Low** | **Port** | TCP 443 |
| **Target** | https://example.com/  https://example.com/sitemap.xml  https://example.com/sitemap.xml.gz  https://example.com/login  https://example.com/backend/  https://example.com/backend/api/v1/  https://example.com/backend/api/  https://example.com/backend.bak  https://example.com/backend.7z  https://example.com/backend.cfg  https://example.com/backend.csv  https://example.com/backend.dump  https://example.com/backend.ini  https://example.com/backend.jar  https://example.com/backend.old  https://example.com/backend.ost  https://example.com/backend.pst  https://example.com/backend.sh  https://example.com/backend.sln  https://example.com/backend.tar  https://example.com/backend.war | | |
| **Detail** | HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response. | | |
| **Impact** | HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks | | |
| **Solution** | It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information | | |
| **Remark** | |  | | --- | | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 3 | **Finding** | Sensitive pages could be cached |
| **Severity** | **Low** | **Port** | TCP 443 |
| **Target** | https://example.com/?password=g00dPa$$w0rDusername=pHqghUme | | |
| **Detail** | One or more pages contain possible sensitive information (e.g., a password parameter) and could be potentially cached. Even in secure SSL channels sensitive data could be stored by intermediary proxies and SSL terminators. To prevent this, a Cache-Control header should be specified. | | |
| **Impact** | Possible sensitive information disclosure. | | |
| **Solution** | Prevent caching by adding "Cache Control: No-store" and "Pragma: no-cache" to the HTTP response header. | | |
| **Remark** | - | | |

# Port Discovery

| **Port** | **Protocol** | **Service** |
| --- | --- | --- |
| 22 | TCP | ssh |
| 80 | TCP | http |
| 110 | TCP | pop3 |
| 143 | TCP | imap-proxy |
| 443 | TCP | https |
| 465 | TCP | ssl/smtp |
| 587 | TCP | smtp |
| 993 | TCP | ssl/imap-proxy |
| 995 | TCP | ssl/pop3 |
| 8443 | TCP | https-alt? |
| 9071 | TCP | ssl/http |

# Appendix

## **8.1 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

### **8.1.1 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

### **8.1.2 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 |

## **8.2 About Acunetix**

Acunetix by Invicti Security is an application security testing tool built to help small mid-size organizations around the world take control of their web security. Acunetix is built to evolve and stay ahead of cybersecurity changes. Acunetix industry-leading dynamic and interactive application security testing (DAST and IAST) technology automates vulnerability management and empowers security teams to uncover more vulnerabilities, reduce false positives, increase productivity, and simplify remediation efforts.

Reference: https://www.acunetix.com/product/, https://www.acunetix.com/about/

### **8.2.1 Acunetix web vulnerabilities**

The following reference link is a list of known web application vulnerabilities that can be automatically detected by Acunetix.

Reference: https://www.acunetix.com/vulnerabilities/web/

### **8.2.2 Acunetix risk score**

Severity is a metric for classifying the level of risk which a security vulnerability poses. The severity level of a vulnerability is assigned based on the security risk posed to an organization should the vulnerability be exploited, as well as the degree of difficulty involved in exploiting it. The result of a successful attack by exploiting a vulnerability could vary from denial of service and information disclosure to a complete compromise of applications or systems. The following provides a description of what the results in this analysis consider to be the impact of each vulnerability severity level.

| **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. |