**Vulnerability Assessment Report**

**For**



**COCO-IDC2 All**

**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 |

|  |  |  |  |
| --- | --- | --- | --- |
| COCO-IDC2 All | | 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 |  | 192.168.9.11 |  | TCP : 22, 80, 443, 5432, 10000 UDP : 123, 161, 10000 |
| 2 |  | 192.168.9.12 |  | TCP : 80, 135, 139, 1237, 2000, 3389, 5060, 5985, 6050, 8000, 8081, 8082, 49152, 49153, 49154, 49155, 49159, 49163, 49208 UDP : 1434 |
| 3 |  | 192.168.9.13 |  | TCP : 135, 139, 445, 1480, 2000, 3389, 5060, 5985, 49152, 49153, 49154, 49155, 49156, 49157 UDP : 137 |
| 4 |  | 192.168.9.14 |  | TCP : 80, 135, 139, 445, 2000, 3389, 5060, 49152, 49153, 49154, 49155, 49156, 49158 UDP : 137 |
| 5 |  | 192.168.9.15 |  | TCP : 21, 80, 135, 139, 445, 2000, 3389, 5060, 49152, 49153, 49154, 49155, 49157, 49158 |
| 6 |  | 192.168.10.3 |  | TCP : 80, 135, 445, 3389, 49152, 49153, 49154, 49156, 49163 |
| 7 |  | 192.168.10.50 |  | TCP : 23 |
| 8 |  | 192.168.10.51 |  | TCP : 23, 80 |
| 9 |  | 192.168.10.52 |  | TCP : 23 |
| 10 |  | 192.168.10.53 |  | TCP : 23, 80 |
| 11 |  | 192.168.10.54 |  | TCP : 21, 23, 80, 502 UDP : 161, 2049, 2050, 2051, 2052, 47808 |
| 12 |  | 192.168.10.55 |  | TCP : 21, 23, 80, 502 UDP : 161, 2049, 2050, 2051, 2052, 47808 |
| 13 |  | 192.168.10.56 |  | TCP : 21, 23, 80, 502 UDP : 161, 2049, 2050, 2051, 2052, 47808 |
| 14 |  | 192.168.10.57 |  | TCP : 21, 23, 80, 502 UDP : 161, 2049, 2050, 2051, 2052, 47808 |
| 15 |  | 192.168.10.58 |  | TCP : 21, 23, 80, 502 UDP : 161, 2049, 2050, 2051, 2052, 47808 |
| 16 |  | 192.168.10.59 |  | TCP : 21, 23, 80, 502 UDP : 161, 2049, 2050, 2051, 2052, 47808 |
| 17 |  | 192.168.10.60 |  | TCP : 21, 23, 80, 502 UDP : 161, 2049, 2050, 2051, 2052, 47808 |
| 18 |  | 192.168.10.61 |  | TCP : 21, 23, 80, 502 UDP : 161, 2049, 2050, 2051, 2052, 47808 |
| 19 |  | 192.168.10.62 |  | TCP : 21, 23, 80, 502 UDP : 161, 2049, 2050, 2051, 2052, 47808 |
| 20 |  | 192.168.10.63 |  | TCP : 21, 23, 80 UDP : 161, 33281, 33795, 34822, 47576, 57588 |
| 21 |  | 192.168.10.64 |  | TCP : 21, 23, 80 UDP : 161, 33281, 33795, 34822, 56592, 61298 |
| 22 |  | 192.168.10.65 |  | TCP : 21, 23, 80 UDP : 161, 33281, 33795, 34822, 37548, 43714 |
| 23 |  | 192.168.10.66 |  | TCP : 21, 23, 80 UDP : 161, 33281, 33795, 34822, 52282, 59944 |
| 24 |  | 192.168.10.67 |  | TCP : 21, 23, 80 UDP : 161, 33281, 33795, 34822, 49701, 50351 |
| 25 |  | 192.168.10.70 |  | TCP : 80, 502 UDP : 161, 39022, 42203, 62512, 64024 |
| 26 |  | 192.168.10.71 |  | TCP : 21, 80, 502 |
| 27 |  | 192.168.10.72 |  | TCP : 80, 502 UDP : 161, 33719, 39690, 41428, 53482 |
| 28 |  | 192.168.10.73 |  | TCP : 21, 80, 502 |
| 29 |  | 192.168.10.74 |  | TCP : 21, 80, 502 |
| 30 |  | 192.168.10.75 |  | TCP : 21, 22, 25, 80, 443 UDP : 123 |
| 31 |  | 192.168.10.76 |  | TCP : 22, 80, 443, 5432 UDP : 67, 123, 161, 162, 6000 |
| 32 |  | 192.168.10.77 |  | TCP : 80, 502 UDP : 161, 34706, 36645, 48995, 59731 |
| 33 |  | 192.168.10.101 |  |  |
| 34 |  | 192.168.10.102 |  |  |
| 35 |  | 192.168.10.103 |  |  |
| 36 |  | 192.168.10.104 |  |  |
| 37 |  | 192.168.10.105 |  |  |
| 38 |  | 192.168.10.106 |  |  |
| 39 |  | 192.168.10.107 |  |  |
| 40 |  | 192.168.10.108 |  |  |
| 41 |  | 192.168.10.109 |  |  |
| 42 |  | 192.168.10.110 |  |  |
| 43 |  | 192.168.10.111 |  |  |
| 44 |  | 192.168.10.112 |  |  |
| 45 |  | 192.168.10.113 |  |  |
| 46 |  | 192.168.10.114 |  |  |
| 47 |  | 192.168.10.115 |  |  |
| 48 |  | 192.168.10.116 |  |  |
| 49 |  | 192.168.10.117 |  |  |
| 50 |  | 192.168.10.118 |  |  |
| 51 |  | 192.168.10.119 |  |  |
| 52 |  | 192.168.10.120 |  |  |
| 53 |  | 192.168.10.121 |  |  |
| 54 |  | 192.168.10.122 |  |  |
| 55 |  | 192.168.10.123 |  |  |
| 56 |  | 192.168.10.124 |  |  |
| 57 |  | 192.168.10.125 |  |  |
| 58 |  | 192.168.10.126 |  |  |
| 59 |  | 192.168.10.127 |  |  |
| 60 |  | 192.168.10.128 |  |  |
| 61 |  | 192.168.10.151 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 62 |  | 192.168.10.152 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 63 |  | 192.168.10.153 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 64 |  | 192.168.10.154 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 65 |  | 192.168.10.155 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 66 |  | 192.168.10.156 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 67 |  | 192.168.10.157 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 68 |  | 192.168.10.158 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 69 |  | 192.168.10.159 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 70 |  | 192.168.10.160 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 71 |  | 192.168.10.161 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 72 |  | 192.168.10.162 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 73 |  | 192.168.10.164 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 74 |  | 192.168.10.165 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 75 |  | 192.168.10.166 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 76 |  | 192.168.10.167 |  | TCP : 80, 554, 8000 UDP : 5353 |
| 77 |  | 192.168.10.169 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 78 |  | 192.168.10.170 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 79 |  | 192.168.10.171 |  | TCP : 80, 554, 8000 UDP : 5353 |
| 80 |  | 192.168.10.172 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 81 |  | 192.168.10.173 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 82 |  | 192.168.10.174 |  | TCP : 80, 554, 8000 UDP : 5353 |
| 83 |  | 192.168.10.175 |  | TCP : 80, 554 UDP : 3702, 5353 |
| 84 |  | 192.168.10.176 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 85 |  | 192.168.10.177 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 86 |  | 192.168.10.178 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 87 |  | 192.168.10.179 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 88 |  | 192.168.10.180 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 89 |  | 192.168.10.181 |  | TCP : 80, 554 UDP : 3702, 5353 |
| 90 |  | 192.168.10.182 |  | TCP : 80, 554, 8000, 9020 UDP : 3702, 5353 |
| 91 |  | 192.168.10.183 |  | TCP : 80, 554, 8000, 9020 UDP : 3702, 5353 |
| 92 |  | 192.168.10.184 |  | TCP : 80, 554, 8000 UDP : 5353 |
| 93 |  | 192.168.11.6 |  | TCP : 80, 135, 139, 445, 3389, 49152, 49153, 49154, 49155, 52748, 53417 UDP : 137, 5355 |
| 94 |  | 192.168.11.7 |  | TCP : 80, 135, 139, 445, 3389, 7070, 8090, 49152, 49153, 49154, 49162, 49163, 49167 UDP : 137, 5355 |
| 95 |  | 192.168.11.9 |  | TCP : 135, 139, 445, 3389, 49152, 49153, 49154, 49192, 49305 UDP : 137, 5355 |
| 96 |  | 192.168.11.24 |  | UDP : 47808 |
| 97 |  | 192.168.11.31 |  | TCP : 80 UDP : 123, 137, 47808 |
| 98 |  | 192.168.11.32 |  | TCP : 23, 80 UDP : 123, 137, 47808 |
| 99 |  | 192.168.11.33 |  | TCP : 80 UDP : 123, 137, 47808 |
| 100 |  | 192.168.11.39 |  | TCP : 80, 135, 139, 445, 1025, 1026, 1027, 1028, 1029, 1032, 1033, 1034, 1433, 1801, 2008, 2103, 2105, 2107, 3389, 5985 UDP : 123, 137, 5355 |
| 101 |  | 192.168.11.41 |  |  |
| 102 |  | 192.168.11.42 |  |  |
| 103 |  | 192.168.11.43 |  |  |
| 104 |  | 192.168.11.44 |  |  |
| 105 |  | 192.168.11.45 |  |  |
| 106 |  | 192.168.11.46 |  |  |
| 107 |  | 192.168.11.47 |  |  |
| 108 |  | 192.168.11.48 |  |  |
| 109 |  | 192.168.11.49 |  |  |
| 110 |  | 192.168.11.50 |  |  |
| 111 |  | 192.168.11.51 |  |  |
| 112 |  | 192.168.11.52 |  |  |
| 113 |  | 192.168.11.53 |  |  |
| 114 |  | 192.168.11.54 |  |  |
| 115 |  | 192.168.11.55 |  |  |
| 116 |  | 192.168.11.56 |  |  |
| 117 |  | 192.168.11.57 |  |  |
| 118 |  | 192.168.11.58 |  |  |
| 119 |  | 192.168.11.59 |  |  |
| 120 |  | 192.168.11.60 |  |  |
| 121 |  | 192.168.11.61 |  |  |
| 122 |  | 192.168.11.62 |  |  |
| 123 |  | 192.168.11.63 |  |  |
| 124 |  | 192.168.11.64 |  |  |
| 125 |  | 192.168.11.65 |  |  |
| 126 |  | 192.168.11.66 |  |  |
| 127 |  | 192.168.11.67 |  |  |
| 128 |  | 192.168.11.68 |  |  |
| 129 |  | 192.168.11.69 |  |  |
| 130 |  | 192.168.11.70 |  |  |
| 131 |  | 192.168.11.71 |  |  |
| 132 |  | 192.168.11.72 |  |  |
| 133 |  | 192.168.11.73 |  |  |
| 134 |  | 192.168.11.74 |  |  |
| 135 |  | 192.168.11.75 |  |  |
| 136 |  | 192.168.11.76 |  |  |
| 137 |  | 192.168.11.77 |  |  |
| 138 |  | 192.168.11.78 |  |  |
| 139 |  | 192.168.11.79 |  |  |
| 140 |  | 192.168.11.80 |  |  |
| 141 |  | 192.168.11.81 |  |  |
| 142 |  | 192.168.11.82 |  |  |
| 143 |  | 192.168.11.83 |  |  |
| 144 |  | 192.168.11.84 |  |  |
| 145 |  | 192.168.11.85 |  |  |
| 146 |  | 192.168.11.86 |  |  |
| 147 |  | 192.168.11.100 |  | TCP : 80, 135, 139, 445, 1480, 2301, 2381, 3389, 49152, 49153, 49154, 49155, 49160, 49172, 49173 UDP : 137, 1434, 5355 |
| 148 |  | 192.168.11.101 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 149 |  | 192.168.11.102 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 150 |  | 192.168.11.103 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 151 |  | 192.168.11.104 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 152 |  | 192.168.11.105 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 153 |  | 192.168.11.106 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 154 |  | 192.168.11.107 |  | TCP : 80, 554, 8080, 8554, 50004 UDP : 1900, 5353 |
| 155 |  | 192.168.11.108 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 156 |  | 192.168.11.109 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 157 |  | 192.168.11.111 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 158 |  | 192.168.11.112 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 159 |  | 192.168.11.113 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 160 |  | 192.168.11.114 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 161 |  | 192.168.11.116 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 162 |  | 192.168.11.117 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 163 |  | 192.168.11.118 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 164 |  | 192.168.11.119 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 165 |  | 192.168.11.120 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 166 |  | 192.168.11.121 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 167 |  | 192.168.11.122 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 168 |  | 192.168.11.123 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 169 |  | 192.168.11.124 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 170 |  | 192.168.11.125 |  | TCP : 80, 443, 554, 8000 UDP : 5353 |
| 171 |  | 192.168.11.126 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 172 |  | 192.168.11.127 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 173 |  | 192.168.11.128 |  | TCP : 80, 554, 8080, 8554, 50004 UDP : 1900, 5353 |
| 174 |  | 192.168.11.129 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 175 |  | 192.168.11.130 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 176 |  | 192.168.11.131 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 177 |  | 192.168.11.132 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 178 |  | 192.168.11.133 |  | TCP : 80, 443, 554, 8000, 8443 UDP : 5353 |
| 179 |  | 192.168.11.134 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 180 |  | 192.168.11.136 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 181 |  | 192.168.11.137 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 182 |  | 192.168.11.138 |  | TCP : 80, 443, 554, 8000, 8443 UDP : 5353 |
| 183 |  | 192.168.11.139 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 184 |  | 192.168.11.140 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 185 |  | 192.168.11.141 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 186 |  | 192.168.11.142 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 187 |  | 192.168.11.143 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 188 |  | 192.168.11.144 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 189 |  | 192.168.11.145 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 190 |  | 192.168.11.146 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 191 |  | 192.168.11.148 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 192 |  | 192.168.11.149 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 193 |  | 192.168.11.150 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 194 |  | 192.168.11.151 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 195 |  | 192.168.11.152 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 196 |  | 192.168.11.153 |  | TCP : 80, 554, 8080, 8554, 50004 UDP : 1900, 5353 |
| 197 |  | 192.168.11.154 |  | TCP : 80, 443, 554, 8000, 8443 UDP : 5353 |
| 198 |  | 192.168.11.155 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 199 |  | 192.168.11.156 |  | TCP : 80, 554, 8000, 9020, 49152 UDP : 1900, 3702, 5353 |
| 200 |  | 192.168.11.157 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 201 |  | 192.168.11.158 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 202 |  | 192.168.11.159 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 203 |  | 192.168.11.160 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 204 |  | 192.168.11.161 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 205 |  | 192.168.11.162 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 206 |  | 192.168.11.163 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 207 |  | 192.168.11.164 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 208 |  | 192.168.11.165 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 209 |  | 192.168.11.166 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 210 |  | 192.168.11.167 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 211 |  | 192.168.11.168 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 212 |  | 192.168.11.169 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 213 |  | 192.168.11.170 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 214 |  | 192.168.11.171 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 215 |  | 192.168.11.172 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 216 |  | 192.168.11.173 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 217 |  | 192.168.11.174 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 218 |  | 192.168.11.175 |  | TCP : 80, 554, 8000, 9020, 49152 UDP : 161, 1900, 3702, 5353 |
| 219 |  | 192.168.11.176 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 220 |  | 192.168.11.177 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 221 |  | 192.168.11.178 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 222 |  | 192.168.11.179 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 223 |  | 192.168.11.180 |  | TCP : 80, 554, 8000, 9020, 49152 UDP : 1900, 5353 |
| 224 |  | 192.168.11.181 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 225 |  | 192.168.11.182 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 226 |  | 192.168.11.183 |  | TCP : 80, 554, 8000, 9020, 49152 UDP : 1900, 3702, 5353 |
| 227 |  | 192.168.11.184 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 228 |  | 192.168.11.185 |  | TCP : 80, 554, 49152 UDP : 1900, 3702, 5353 |
| 229 |  | 192.168.11.189 |  | TCP : 135, 139, 445, 5150, 49152, 49153, 49154, 49155, 49222, 49241 UDP : 137, 5355 |

## **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**

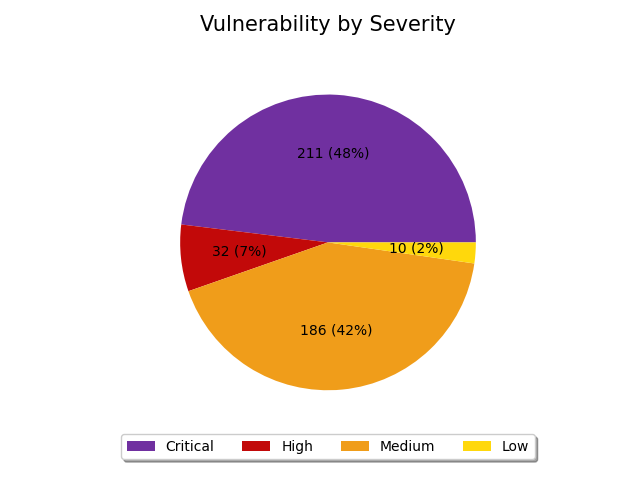


Figure 4: Summary by Severity of Infrastructure Vulnerability Assessment

### **5.2.2 Vulnerability by Target**

| **No.** | **Domain/Server Name** | **IP Address** | **Critical** | **High** | **Medium** | **Low** | **Total** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | - | 192.168.9.11 | 0 | 1 | 6 | 3 | 10 |
| 2 | - | 192.168.9.12 | 1 | 2 | 21 | 2 | 26 |
| 3 | - | 192.168.9.13 | 1 | 1 | 15 | 0 | 17 |
| 4 | - | 192.168.9.14 | 1 | 0 | 1 | 0 | 2 |
| 5 | - | 192.168.9.15 | 0 | 0 | 0 | 0 | 0 |
| 6 | - | 192.168.10.3 | 2 | 1 | 7 | 0 | 10 |
| 7 | - | 192.168.10.50 | 0 | 0 | 0 | 0 | 0 |
| 8 | - | 192.168.10.51 | 0 | 0 | 0 | 0 | 0 |
| 9 | - | 192.168.10.52 | 0 | 0 | 0 | 0 | 0 |
| 10 | - | 192.168.10.53 | 0 | 0 | 0 | 0 | 0 |
| 11 | - | 192.168.10.54 | 0 | 0 | 2 | 0 | 2 |
| 12 | - | 192.168.10.55 | 0 | 0 | 2 | 0 | 2 |
| 13 | - | 192.168.10.56 | 0 | 0 | 2 | 0 | 2 |
| 14 | - | 192.168.10.57 | 0 | 0 | 2 | 0 | 2 |
| 15 | - | 192.168.10.58 | 0 | 0 | 2 | 0 | 2 |
| 16 | - | 192.168.10.59 | 0 | 0 | 2 | 0 | 2 |
| 17 | - | 192.168.10.60 | 0 | 0 | 2 | 0 | 2 |
| 18 | - | 192.168.10.61 | 0 | 0 | 2 | 0 | 2 |
| 19 | - | 192.168.10.62 | 0 | 0 | 2 | 0 | 2 |
| 20 | - | 192.168.10.63 | 0 | 0 | 0 | 0 | 0 |
| 21 | - | 192.168.10.64 | 0 | 0 | 0 | 0 | 0 |
| 22 | - | 192.168.10.65 | 0 | 0 | 0 | 0 | 0 |
| 23 | - | 192.168.10.66 | 0 | 0 | 0 | 0 | 0 |
| 24 | - | 192.168.10.67 | 0 | 0 | 0 | 0 | 0 |
| 25 | - | 192.168.10.70 | 0 | 0 | 1 | 0 | 1 |
| 26 | - | 192.168.10.71 | 0 | 0 | 2 | 0 | 2 |
| 27 | - | 192.168.10.72 | 0 | 0 | 2 | 0 | 2 |
| 28 | - | 192.168.10.73 | 1 | 0 | 0 | 0 | 1 |
| 29 | - | 192.168.10.74 | 0 | 0 | 2 | 0 | 2 |
| 30 | - | 192.168.10.75 | 0 | 0 | 3 | 0 | 3 |
| 31 | - | 192.168.10.76 | 0 | 1 | 4 | 1 | 6 |
| 32 | - | 192.168.10.77 | 0 | 0 | 2 | 0 | 2 |
| 33 | - | 192.168.10.101 | 0 | 0 | 0 | 0 | 0 |
| 34 | - | 192.168.10.102 | 0 | 0 | 0 | 0 | 0 |
| 35 | - | 192.168.10.103 | 0 | 0 | 0 | 0 | 0 |
| 36 | - | 192.168.10.104 | 0 | 0 | 0 | 0 | 0 |
| 37 | - | 192.168.10.105 | 0 | 0 | 0 | 0 | 0 |
| 38 | - | 192.168.10.106 | 0 | 0 | 0 | 0 | 0 |
| 39 | - | 192.168.10.107 | 0 | 0 | 0 | 0 | 0 |
| 40 | - | 192.168.10.108 | 0 | 0 | 0 | 0 | 0 |
| 41 | - | 192.168.10.109 | 0 | 0 | 0 | 0 | 0 |
| 42 | - | 192.168.10.110 | 0 | 0 | 0 | 0 | 0 |
| 43 | - | 192.168.10.111 | 0 | 0 | 0 | 0 | 0 |
| 44 | - | 192.168.10.112 | 0 | 0 | 0 | 0 | 0 |
| 45 | - | 192.168.10.113 | 0 | 0 | 0 | 0 | 0 |
| 46 | - | 192.168.10.114 | 0 | 0 | 0 | 0 | 0 |
| 47 | - | 192.168.10.115 | 0 | 0 | 0 | 0 | 0 |
| 48 | - | 192.168.10.116 | 0 | 0 | 0 | 0 | 0 |
| 49 | - | 192.168.10.117 | 0 | 0 | 0 | 0 | 0 |
| 50 | - | 192.168.10.118 | 0 | 0 | 0 | 0 | 0 |
| 51 | - | 192.168.10.119 | 0 | 0 | 0 | 0 | 0 |
| 52 | - | 192.168.10.120 | 0 | 0 | 0 | 0 | 0 |
| 53 | - | 192.168.10.121 | 0 | 0 | 0 | 0 | 0 |
| 54 | - | 192.168.10.122 | 0 | 0 | 0 | 0 | 0 |
| 55 | - | 192.168.10.123 | 0 | 0 | 0 | 0 | 0 |
| 56 | - | 192.168.10.124 | 0 | 0 | 0 | 0 | 0 |
| 57 | - | 192.168.10.125 | 0 | 0 | 0 | 0 | 0 |
| 58 | - | 192.168.10.126 | 0 | 0 | 0 | 0 | 0 |
| 59 | - | 192.168.10.127 | 0 | 0 | 0 | 0 | 0 |
| 60 | - | 192.168.10.128 | 0 | 0 | 0 | 0 | 0 |
| 61 | - | 192.168.10.151 | 2 | 0 | 0 | 0 | 2 |
| 62 | - | 192.168.10.152 | 2 | 0 | 0 | 0 | 2 |
| 63 | - | 192.168.10.153 | 2 | 0 | 0 | 0 | 2 |
| 64 | - | 192.168.10.154 | 2 | 0 | 0 | 0 | 2 |
| 65 | - | 192.168.10.155 | 2 | 0 | 0 | 0 | 2 |
| 66 | - | 192.168.10.156 | 2 | 0 | 0 | 0 | 2 |
| 67 | - | 192.168.10.157 | 2 | 0 | 0 | 0 | 2 |
| 68 | - | 192.168.10.158 | 2 | 0 | 0 | 0 | 2 |
| 69 | - | 192.168.10.159 | 2 | 0 | 0 | 0 | 2 |
| 70 | - | 192.168.10.160 | 2 | 0 | 0 | 0 | 2 |
| 71 | - | 192.168.10.161 | 2 | 0 | 0 | 0 | 2 |
| 72 | - | 192.168.10.162 | 2 | 0 | 0 | 0 | 2 |
| 73 | - | 192.168.10.164 | 2 | 0 | 0 | 0 | 2 |
| 74 | - | 192.168.10.165 | 2 | 0 | 0 | 0 | 2 |
| 75 | - | 192.168.10.166 | 2 | 0 | 0 | 0 | 2 |
| 76 | - | 192.168.10.167 | 0 | 0 | 0 | 0 | 0 |
| 77 | - | 192.168.10.169 | 2 | 0 | 0 | 0 | 2 |
| 78 | - | 192.168.10.170 | 2 | 0 | 0 | 0 | 2 |
| 79 | - | 192.168.10.171 | 0 | 0 | 0 | 0 | 0 |
| 80 | - | 192.168.10.172 | 2 | 0 | 0 | 0 | 2 |
| 81 | - | 192.168.10.173 | 2 | 0 | 0 | 0 | 2 |
| 82 | - | 192.168.10.174 | 0 | 0 | 0 | 0 | 0 |
| 83 | - | 192.168.10.175 | 0 | 0 | 0 | 0 | 0 |
| 84 | - | 192.168.10.176 | 2 | 0 | 0 | 0 | 2 |
| 85 | - | 192.168.10.177 | 2 | 0 | 0 | 0 | 2 |
| 86 | - | 192.168.10.178 | 2 | 0 | 0 | 0 | 2 |
| 87 | - | 192.168.10.179 | 2 | 0 | 0 | 0 | 2 |
| 88 | - | 192.168.10.180 | 2 | 0 | 0 | 0 | 2 |
| 89 | - | 192.168.10.181 | 0 | 0 | 0 | 0 | 0 |
| 90 | - | 192.168.10.182 | 0 | 0 | 0 | 0 | 0 |
| 91 | - | 192.168.10.183 | 0 | 0 | 0 | 0 | 0 |
| 92 | - | 192.168.10.184 | 0 | 0 | 0 | 0 | 0 |
| 93 | - | 192.168.11.6 | 1 | 4 | 9 | 0 | 14 |
| 94 | - | 192.168.11.7 | 2 | 1 | 14 | 1 | 18 |
| 95 | - | 192.168.11.9 | 3 | 2 | 7 | 0 | 12 |
| 96 | - | 192.168.11.24 | 0 | 0 | 0 | 0 | 0 |
| 97 | - | 192.168.11.31 | 0 | 0 | 0 | 0 | 0 |
| 98 | - | 192.168.11.32 | 0 | 0 | 0 | 0 | 0 |
| 99 | - | 192.168.11.33 | 0 | 0 | 0 | 0 | 0 |
| 100 | - | 192.168.11.39 | 1 | 2 | 16 | 1 | 20 |
| 101 | - | 192.168.11.41 | 0 | 0 | 0 | 0 | 0 |
| 102 | - | 192.168.11.42 | 0 | 0 | 0 | 0 | 0 |
| 103 | - | 192.168.11.43 | 0 | 0 | 0 | 0 | 0 |
| 104 | - | 192.168.11.44 | 0 | 0 | 0 | 0 | 0 |
| 105 | - | 192.168.11.45 | 0 | 0 | 0 | 0 | 0 |
| 106 | - | 192.168.11.46 | 0 | 0 | 0 | 0 | 0 |
| 107 | - | 192.168.11.47 | 0 | 0 | 0 | 0 | 0 |
| 108 | - | 192.168.11.48 | 0 | 0 | 0 | 0 | 0 |
| 109 | - | 192.168.11.49 | 0 | 0 | 0 | 0 | 0 |
| 110 | - | 192.168.11.50 | 0 | 0 | 0 | 0 | 0 |
| 111 | - | 192.168.11.51 | 0 | 0 | 0 | 0 | 0 |
| 112 | - | 192.168.11.52 | 0 | 0 | 0 | 0 | 0 |
| 113 | - | 192.168.11.53 | 0 | 0 | 0 | 0 | 0 |
| 114 | - | 192.168.11.54 | 0 | 0 | 0 | 0 | 0 |
| 115 | - | 192.168.11.55 | 0 | 0 | 0 | 0 | 0 |
| 116 | - | 192.168.11.56 | 0 | 0 | 0 | 0 | 0 |
| 117 | - | 192.168.11.57 | 0 | 0 | 0 | 0 | 0 |
| 118 | - | 192.168.11.58 | 0 | 0 | 0 | 0 | 0 |
| 119 | - | 192.168.11.59 | 0 | 0 | 0 | 0 | 0 |
| 120 | - | 192.168.11.60 | 0 | 0 | 0 | 0 | 0 |
| 121 | - | 192.168.11.61 | 0 | 0 | 0 | 0 | 0 |
| 122 | - | 192.168.11.62 | 0 | 0 | 0 | 0 | 0 |
| 123 | - | 192.168.11.63 | 0 | 0 | 0 | 0 | 0 |
| 124 | - | 192.168.11.64 | 0 | 0 | 0 | 0 | 0 |
| 125 | - | 192.168.11.65 | 0 | 0 | 0 | 0 | 0 |
| 126 | - | 192.168.11.66 | 0 | 0 | 0 | 0 | 0 |
| 127 | - | 192.168.11.67 | 0 | 0 | 0 | 0 | 0 |
| 128 | - | 192.168.11.68 | 0 | 0 | 0 | 0 | 0 |
| 129 | - | 192.168.11.69 | 0 | 0 | 0 | 0 | 0 |
| 130 | - | 192.168.11.70 | 0 | 0 | 0 | 0 | 0 |
| 131 | - | 192.168.11.71 | 0 | 0 | 0 | 0 | 0 |
| 132 | - | 192.168.11.72 | 0 | 0 | 0 | 0 | 0 |
| 133 | - | 192.168.11.73 | 0 | 0 | 0 | 0 | 0 |
| 134 | - | 192.168.11.74 | 0 | 0 | 0 | 0 | 0 |
| 135 | - | 192.168.11.75 | 0 | 0 | 0 | 0 | 0 |
| 136 | - | 192.168.11.76 | 0 | 0 | 0 | 0 | 0 |
| 137 | - | 192.168.11.77 | 0 | 0 | 0 | 0 | 0 |
| 138 | - | 192.168.11.78 | 0 | 0 | 0 | 0 | 0 |
| 139 | - | 192.168.11.79 | 0 | 0 | 0 | 0 | 0 |
| 140 | - | 192.168.11.80 | 0 | 0 | 0 | 0 | 0 |
| 141 | - | 192.168.11.81 | 0 | 0 | 0 | 0 | 0 |
| 142 | - | 192.168.11.82 | 0 | 0 | 0 | 0 | 0 |
| 143 | - | 192.168.11.83 | 0 | 0 | 0 | 0 | 0 |
| 144 | - | 192.168.11.84 | 0 | 0 | 0 | 0 | 0 |
| 145 | - | 192.168.11.85 | 0 | 0 | 0 | 0 | 0 |
| 146 | - | 192.168.11.86 | 0 | 0 | 0 | 0 | 0 |
| 147 | - | 192.168.11.100 | 8 | 11 | 38 | 2 | 59 |
| 148 | - | 192.168.11.101 | 2 | 0 | 0 | 0 | 2 |
| 149 | - | 192.168.11.102 | 2 | 0 | 0 | 0 | 2 |
| 150 | - | 192.168.11.103 | 2 | 0 | 0 | 0 | 2 |
| 151 | - | 192.168.11.104 | 2 | 0 | 0 | 0 | 2 |
| 152 | - | 192.168.11.105 | 2 | 0 | 0 | 0 | 2 |
| 153 | - | 192.168.11.106 | 2 | 0 | 0 | 0 | 2 |
| 154 | - | 192.168.11.107 | 0 | 0 | 0 | 0 | 0 |
| 155 | - | 192.168.11.108 | 2 | 0 | 0 | 0 | 2 |
| 156 | - | 192.168.11.109 | 2 | 0 | 0 | 0 | 2 |
| 157 | - | 192.168.11.111 | 2 | 0 | 0 | 0 | 2 |
| 158 | - | 192.168.11.112 | 2 | 0 | 0 | 0 | 2 |
| 159 | - | 192.168.11.113 | 2 | 0 | 0 | 0 | 2 |
| 160 | - | 192.168.11.114 | 2 | 0 | 0 | 0 | 2 |
| 161 | - | 192.168.11.116 | 2 | 0 | 0 | 0 | 2 |
| 162 | - | 192.168.11.117 | 2 | 0 | 0 | 0 | 2 |
| 163 | - | 192.168.11.118 | 2 | 0 | 0 | 0 | 2 |
| 164 | - | 192.168.11.119 | 2 | 0 | 0 | 0 | 2 |
| 165 | - | 192.168.11.120 | 2 | 0 | 0 | 0 | 2 |
| 166 | - | 192.168.11.121 | 2 | 0 | 0 | 0 | 2 |
| 167 | - | 192.168.11.122 | 2 | 0 | 0 | 0 | 2 |
| 168 | - | 192.168.11.123 | 2 | 0 | 0 | 0 | 2 |
| 169 | - | 192.168.11.124 | 2 | 0 | 0 | 0 | 2 |
| 170 | - | 192.168.11.125 | 0 | 0 | 0 | 0 | 0 |
| 171 | - | 192.168.11.126 | 2 | 0 | 0 | 0 | 2 |
| 172 | - | 192.168.11.127 | 2 | 0 | 0 | 0 | 2 |
| 173 | - | 192.168.11.128 | 0 | 0 | 1 | 0 | 1 |
| 174 | - | 192.168.11.129 | 2 | 0 | 0 | 0 | 2 |
| 175 | - | 192.168.11.130 | 2 | 0 | 0 | 0 | 2 |
| 176 | - | 192.168.11.131 | 2 | 0 | 0 | 0 | 2 |
| 177 | - | 192.168.11.132 | 2 | 0 | 0 | 0 | 2 |
| 178 | - | 192.168.11.133 | 0 | 0 | 6 | 0 | 6 |
| 179 | - | 192.168.11.134 | 2 | 0 | 0 | 0 | 2 |
| 180 | - | 192.168.11.136 | 2 | 0 | 0 | 0 | 2 |
| 181 | - | 192.168.11.137 | 2 | 0 | 0 | 0 | 2 |
| 182 | - | 192.168.11.138 | 0 | 0 | 4 | 0 | 4 |
| 183 | - | 192.168.11.139 | 2 | 0 | 0 | 0 | 2 |
| 184 | - | 192.168.11.140 | 2 | 0 | 0 | 0 | 2 |
| 185 | - | 192.168.11.141 | 2 | 0 | 0 | 0 | 2 |
| 186 | - | 192.168.11.142 | 2 | 0 | 0 | 0 | 2 |
| 187 | - | 192.168.11.143 | 2 | 0 | 0 | 0 | 2 |
| 188 | - | 192.168.11.144 | 2 | 0 | 0 | 0 | 2 |
| 189 | - | 192.168.11.145 | 2 | 0 | 0 | 0 | 2 |
| 190 | - | 192.168.11.146 | 2 | 0 | 0 | 0 | 2 |
| 191 | - | 192.168.11.148 | 2 | 0 | 0 | 0 | 2 |
| 192 | - | 192.168.11.149 | 2 | 0 | 0 | 0 | 2 |
| 193 | - | 192.168.11.150 | 2 | 0 | 0 | 0 | 2 |
| 194 | - | 192.168.11.151 | 2 | 0 | 0 | 0 | 2 |
| 195 | - | 192.168.11.152 | 2 | 0 | 0 | 0 | 2 |
| 196 | - | 192.168.11.153 | 0 | 0 | 1 | 0 | 1 |
| 197 | - | 192.168.11.154 | 0 | 0 | 4 | 0 | 4 |
| 198 | - | 192.168.11.155 | 2 | 0 | 0 | 0 | 2 |
| 199 | - | 192.168.11.156 | 0 | 0 | 0 | 0 | 0 |
| 200 | - | 192.168.11.157 | 2 | 0 | 0 | 0 | 2 |
| 201 | - | 192.168.11.158 | 2 | 0 | 0 | 0 | 2 |
| 202 | - | 192.168.11.159 | 2 | 0 | 0 | 0 | 2 |
| 203 | - | 192.168.11.160 | 2 | 0 | 0 | 0 | 2 |
| 204 | - | 192.168.11.161 | 2 | 0 | 0 | 0 | 2 |
| 205 | - | 192.168.11.162 | 2 | 0 | 0 | 0 | 2 |
| 206 | - | 192.168.11.163 | 2 | 0 | 0 | 0 | 2 |
| 207 | - | 192.168.11.164 | 2 | 0 | 0 | 0 | 2 |
| 208 | - | 192.168.11.165 | 2 | 0 | 0 | 0 | 2 |
| 209 | - | 192.168.11.166 | 2 | 0 | 0 | 0 | 2 |
| 210 | - | 192.168.11.167 | 2 | 0 | 0 | 0 | 2 |
| 211 | - | 192.168.11.168 | 2 | 0 | 0 | 0 | 2 |
| 212 | - | 192.168.11.169 | 2 | 0 | 0 | 0 | 2 |
| 213 | - | 192.168.11.170 | 2 | 0 | 0 | 0 | 2 |
| 214 | - | 192.168.11.171 | 2 | 0 | 0 | 0 | 2 |
| 215 | - | 192.168.11.172 | 2 | 0 | 0 | 0 | 2 |
| 216 | - | 192.168.11.173 | 2 | 0 | 0 | 0 | 2 |
| 217 | - | 192.168.11.174 | 2 | 0 | 0 | 0 | 2 |
| 218 | - | 192.168.11.175 | 0 | 2 | 0 | 0 | 2 |
| 219 | - | 192.168.11.176 | 2 | 0 | 0 | 0 | 2 |
| 220 | - | 192.168.11.177 | 2 | 0 | 0 | 0 | 2 |
| 221 | - | 192.168.11.178 | 2 | 0 | 0 | 0 | 2 |
| 222 | - | 192.168.11.179 | 2 | 0 | 0 | 0 | 2 |
| 223 | - | 192.168.11.180 | 0 | 1 | 0 | 0 | 1 |
| 224 | - | 192.168.11.181 | 2 | 0 | 0 | 0 | 2 |
| 225 | - | 192.168.11.182 | 2 | 0 | 0 | 0 | 2 |
| 226 | - | 192.168.11.183 | 0 | 1 | 0 | 0 | 1 |
| 227 | - | 192.168.11.184 | 2 | 0 | 0 | 0 | 2 |
| 228 | - | 192.168.11.185 | 2 | 0 | 0 | 0 | 2 |
| 229 | - | 192.168.11.189 | 2 | 2 | 2 | 0 | 6 |
| **Total** | | | 211 | 32 | 186 | 10 | 439 |

## **5.3 Infrastructure Vulnerability Detail**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 1 | **Finding** | HP System Management Homepage 7.0 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 2381 |
| **Target** | 192.168.11.100(2381) | | |
| **Detail** | According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote host is earlier than 7.0. As such, it is reportedly affected by the following vulnerabilities :   - An error exists in the 'generate-id' function in the  bundled libxslt library that can allow disclosure of  heap memory addresses. (CVE-2011-0195)   - An unspecified input validation error exists and can  allow cross-site request forgery attacks. (CVE-2011-3846)   - Unspecified errors can allow attackers to carry out   denial of service attacks via unspecified vectors.  (CVE-2012-0135, CVE-2012-1993)   - The bundled version of PHP contains multiple  vulnerabilities. (CVE-2010-3436, CVE-2010-4409,  CVE-2010-4645, CVE-2011-1148, CVE-2011-1153,  CVE-2011-1464, CVE-2011-1467, CVE-2011-1468,  CVE-2011-1470, CVE-2011-1471, CVE-2011-1938,  CVE-2011-2202, CVE-2011-2483, CVE-2011-3182,  CVE-2011-3189, CVE-2011-3267, CVE-2011-3268)   - The bundled version of Apache contains multiple  vulnerabilities. (CVE-2010-1452, CVE-2010-1623,  CVE-2010-2068, CVE-2010-2791, CVE-2011-0419,  CVE-2011-1928, CVE-2011-3192, CVE-2011-3348,  CVE-2011-3368, CVE-2011-3639)   - OpenSSL libraries are contained in several of the  bundled components and contain multiple vulnerabilities.  (CVE-2011-0014, CVE-2011-1468, CVE-2011-1945,  CVE-2011-3207,CVE-2011-3210)   - Curl libraries are contained in several of the bundled  components and contain multiple vulnerabilities.  (CVE-2009-0037, CVE-2010-0734, CVE-2011-2192) | | |
| **Solution** | Upgrade to HP System Management Homepage 7.0 or later. | | |
| **Remark** | http://www.nessus.org/u?106ec533 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 2 | **Finding** | HP System Management Homepage 7.1.1 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 2381 |
| **Target** | 192.168.11.100(2381) | | |
| **Detail** | According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote host is earlier than 7.1.1 and is, therefore, reportedly affected by the following vulnerabilities :   - The bundled version of the libxml2 library contains  multiple vulnerabilities. (CVE-2011-1944, CVE-2011-2821,  CVE-2011-2834)   - The bundled version of PHP contains multiple  vulnerabilities. (CVE-2011-3379, CVE-2011-4153,   CVE-2011-4885, CVE-2012-1823, CVE-2012-0057,   CVE-2012-0830)   - The bundled version of the Apache HTTP Server contains  multiple vulnerabilities. (CVE-2011-3607, CVE-2011-4317,  CVE-2011-4415, CVE-2012-0021, CVE-2012-0031,   CVE-2012-0053)   - An issue exists in the 'include/iniset.php' script in  the embedded RoundCube Webmail version that could lead  to a denial of service. (CVE-2011-4078)   - The bundled version of OpenSSL contains multiple   vulnerabilities. (CVE-2011-4108, CVE-2011-4576,  CVE-2011-4577, CVE-2011-4619, CVE-2012-0027,  CVE-2012-1165)   - The bundled version of curl and libcurl does not   properly consider special characters during extraction  of a pathname from a URL. (CVE-2012-0036)    - An off autocomplete attribute does not exist for   unspecified form fields, which makes it easier for   remote attackers to obtain access by leveraging an  unattended workstation. (CVE-2012-2012)   - An unspecified vulnerability exists that could allow a  remote attacker to cause a denial of service, or  possibly obtain sensitive information or modify data.  (CVE-2012-2013)   - An unspecified vulnerability exists related to improper  input validation. (CVE-2012-2014)   - An unspecified vulnerability allows remote,   unauthenticated users to gain privileges and obtain   sensitive information. (CVE-2012-2015)   - An unspecified vulnerability allows local users to  obtain sensitive information via unknown vectors.  (CVE-2012-2016) | | |
| **Solution** | Upgrade to HP System Management Homepage 7.1.1 or later. | | |
| **Remark** | http://www.nessus.org/u?d07467b6 https://www.securityfocus.com/archive/1/523320/30/0/threaded | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 3 | **Finding** | Microsoft SQL Server Unsupported Version Detection (remote check) |
| **Severity** | Critical | **Port** | TCP: 1433, 49160, 49208 |
| **Target** | 192.168.9.12(49208), 192.168.11.39(1433), 192.168.11.100(49160) | | |
| **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.** | 4 | **Finding** | MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check) |
| **Severity** | Critical | **Port** | TCP: 3389 |
| **Target** | 192.168.10.3(3389), 192.168.11.9(3389), 192.168.11.100(3389) | | |
| **Detail** | The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the Secure Channel (Schannel) security package. An attacker can exploit this issue by sending specially crafted packets to a Windows server.  Note that this plugin sends a client Certificate TLS handshake message followed by a CertificateVerify message. Some Windows hosts will close the connection upon receiving a client certificate for which it did not ask for with a CertificateRequest message. In this case, the plugin cannot proceed to detect the vulnerability as the CertificateVerify message cannot be sent. | | |
| **Solution** | Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2. | | |
| **Remark** | http://www.nessus.org/u?64e97902 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 5 | **Finding** | HP System Management Homepage 7.5.4 Multiple Vulnerabilities (Logjam) |
| **Severity** | Critical | **Port** | TCP: 2381 |
| **Target** | 192.168.11.100(2381) | | |
| **Detail** | According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server is a version prior to 7.5.4. It is, therefore, affected by the following vulnerabilities :   - A denial of service vulnerability exists when processing  an ECParameters structure due to an infinite loop that  occurs when a specified curve is over a malformed binary  polynomial field. A remote attacker can exploit this to  perform a denial of service against any system that  processes public keys, certificate requests, or  certificates. This includes TLS clients and TLS servers  with client authentication enabled. (CVE-2015-1788)    - A denial of service vulnerability exists due to improper  validation of the content and length of the ASN1\_TIME  string by the X509\_cmp\_time() function. A remote  attacker can exploit this, via a malformed certificate  and CRLs of various sizes, to cause a segmentation  fault, resulting in a denial of service condition. TLS  clients that verify CRLs are affected. TLS clients and  servers with client authentication enabled may be  affected if they use custom verification callbacks.  (CVE-2015-1789)   - A NULL pointer dereference flaw exists in the PKCS#7  parsing code due to incorrect handling of missing inner  'EncryptedContent'. This allows a remote attacker, via  specially crafted ASN.1-encoded PKCS#7 blobs with  missing content, to cause a denial of service condition  or other potential unspecified impacts. (CVE-2015-1790)   - A double-free error exists due to a race condition that  occurs when a NewSessionTicket is received by a  multi-threaded client when attempting to reuse a  previous ticket. (CVE-2015-1791)   - A denial of service vulnerability exists in the CMS code  due to an infinite loop that occurs when verifying a  signedData message. A remote attacker can exploit this  to cause a denial of service condition. (CVE-2015-1792)   - A certificate validation bypass vulnerability exists in  the Security:Encryption subcomponent due to a flaw in  the X509\_verify\_cert() function in x509\_vfy.c that is  triggered when locating alternate certificate chains  when the first attempt to build such a chain fails. A  remote attacker can exploit this, by using a valid leaf  certificate as a certificate authority (CA), to issue  invalid certificates that will bypass authentication.  (CVE-2015-1793)   - A cross-request authentication bypass vulnerability  exists in libcurl due to the use of an existing,  authenticated connection when performing a subsequent  unauthenticated NTLM HTTP request. An attacker can  exploit this to bypass authentication mechanisms.  (CVE-2015-3143)   - A denial of service vulnerability exists in libcurl due  to a flaw in the sanitize\_cookie\_path() function that is  triggered when handling a cookie path element that  consists of a single double-quote. An attacker can  exploit this to cause the application to crash.  (CVE-2015-3145)   - A cross-request authentication bypass vulnerability  exists in libcurl due to a flaw that is triggered when a  request is 'Negotiate' authenticated, which can cause  the program to treat the entire connection as  authenticated rather than just that specific request. An  attacker can exploit this to bypass authentication  mechanisms for subsequent requests. (CVE-2015-3148)   - A man-in-the-middle vulnerability, known as Logjam,  exists due to a flaw in the SSL/TLS protocol. A remote  attacker can exploit this flaw to downgrade connections  using ephemeral Diffie-Hellman key exchange to 512-bit  export-grade cryptography. (CVE-2015-4000)   - A flaw exists in the multipart\_buffer\_headers() function  in rfc1867.c due to improper handling of  multipart/form-data in HTTP requests. A remote attacker  can exploit this flaw to cause a consumption of CPU  resources, resulting in a denial of service condition.  (CVE-2015-4024)   - An unspecified flaw exists that allows an authenticated,  remote attacker to impact confidentiality and integrity.  (CVE-2016-1993)   - An unspecified information disclosure vulnerability  exists that allows an authenticated, remote attacker to  gain unauthorized access to information. (CVE-2016-1994)   - An unspecified remote code execution vulnerability  exists that allows an unauthenticated, remote attacker  to take complete control of the system. (CVE-2016-1995)   - An unspecified flaw exists that allows a local attacker  to impact confidentiality and integrity. (CVE-2016-1996) | | |
| **Solution** | Upgrade to HP System Management Homepage (SMH) version 7.5.4 or later. | | |
| **Remark** | http://www.nessus.org/u?d91095a9 https://weakdh.org/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 6 | **Finding** | HP System Management Homepage Multiple Vulnerabilities (HPSBMU03593) |
| **Severity** | Critical | **Port** | TCP: 2381 |
| **Target** | 192.168.11.100(2381) | | |
| **Detail** | According to its banner, the version of HP System Management Homepage (SMH) hosted on the remote web server is affected by the following vulnerabilities :   - A denial of service vulnerability exists in the Apache  HTTP Server due to the lack of the mod\_reqtimeout  module. An unauthenticated, remote attacker can exploit  this, via a saturation of partial HTTP requests, to  cause a daemon outage. (CVE-2007-6750)   - A cross-site scripting (XSS) vulnerability exists in  jQuery when using location.hash to select elements. An  unauthenticated, remote attacker can exploit this, via  a specially crafted tag, to inject arbitrary script  code or HTML into the user's browser session.  (CVE-2011-4969)   - A NULL pointer dereference flaw exists in file  rsa\_ameth.c due to improper handling of ASN.1 signatures  that are missing the PSS parameter. A remote attacker  can exploit this to cause the signature verification  routine to crash, resulting in a denial of service  condition. (CVE-2015-3194)   - A flaw exists in the ASN1\_TFLG\_COMBINE implementation in  file tasn\_dec.c related to handling malformed  X509\_ATTRIBUTE structures. A remote attacker can exploit  this to cause a memory leak by triggering a decoding  failure in a PKCS#7 or CMS application, resulting in a  denial of service. (CVE-2015-3195)   - An out-of-bounds read error exists in cURL and libcurl  within the smb\_request\_state() function due to improper  bounds checking. An unauthenticated, remote attacker  can exploit this, using a malicious SMB server and  crafted length and offset values, to disclose sensitive  memory information or to cause a denial of service  condition. (CVE-2015-3237)   - A flaw exists in libxslt in the xsltStylePreCompute()  function within file preproc.c due to a failure to check  if the parent node is an element. An unauthenticated,  remote attacker can exploit this, via a specially  crafted XML file, to cause a denial of service  condition. (CVE-2015-7995)   - An infinite loop condition exists in the xz\_decomp()  function within file xzlib.c when handling xz compressed  XML content due to a failure to detect compression  errors. An unauthenticated, remote attacker can exploit  this, via specially crafted XML data, to cause a denial  of service condition. (CVE-2015-8035)   - A double-free error exists due to improper validation of  user-supplied input when parsing malformed DSA private  keys. A remote attacker can exploit this to corrupt  memory, resulting in a denial of service condition or  the execution of arbitrary code. (CVE-2016-0705)   - An out-of-bounds read error exists in the fmtstr()  function within file crypto/bio/b\_print.c when printing  very long strings due to a failure to properly calculate  string lengths. An unauthenticated, remote attacker can  exploit this, via a long string, to cause a denial of  service condition, as demonstrated by a large amount of  ASN.1 data. (CVE-2016-0799)   - An unspecified flaw exists that allows a local attacker  to impact the confidentiality and integrity of the  system. No other details are available. (CVE-2016-2015)   - A flaw exists in the doapr\_outch() function within file  crypto/bio/b\_print.c due to a failure to verify that a  certain memory allocation succeeds. An unauthenticated,  remote attacker can exploit this, via a long string,  to cause a denial of service condition, as demonstrated  by a large amount of ASN.1 data. (CVE-2016-2842) | | |
| **Solution** | Upgrade to HP System Management Homepage version 7.5.5 or later. | | |
| **Remark** | http://www.nessus.org/u?8d21af70 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 7 | **Finding** | Unsupported Windows OS (remote) |
| **Severity** | Critical | **Port** | TCP: 0 |
| **Target** | 192.168.9.13(0), 192.168.9.14(0), 192.168.10.3(0), 192.168.11.6(0), 192.168.11.7(0), 192.168.11.9(0), 192.168.11.100(0), 192.168.11.189(0) | | |
| **Detail** | The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities. | | |
| **Solution** | Upgrade to a supported service pack or operating system | | |
| **Remark** | https://support.microsoft.com/en-us/lifecycle | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 8 | **Finding** | Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check) |
| **Severity** | Critical | **Port** | TCP: 3389 |
| **Target** | 192.168.11.7(3389), 192.168.11.100(3389) | | |
| **Detail** | The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code. | | |
| **Solution** | Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2. | | |
| **Remark** | http://www.nessus.org/u?577af692 http://www.nessus.org/u?8e4e0b74 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 9 | **Finding** | MiniUPnP 1.4 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 49152  UDP: 1900 |
| **Target** | 192.168.10.151(1900, 49152), 192.168.10.152(1900, 49152), 192.168.10.153(1900, 49152), 192.168.10.154(1900, 49152), 192.168.10.155(1900, 49152), 192.168.10.156(1900, 49152), 192.168.10.157(1900, 49152), 192.168.10.158(1900, 49152), 192.168.10.159(1900, 49152), 192.168.10.160(1900, 49152), 192.168.10.161(1900, 49152), 192.168.10.162(1900, 49152), 192.168.10.164(1900, 49152), 192.168.10.165(1900, 49152), 192.168.10.166(1900, 49152), 192.168.10.169(1900, 49152), 192.168.10.170(1900, 49152), 192.168.10.172(1900, 49152), 192.168.10.173(1900, 49152), 192.168.10.176(1900, 49152), 192.168.10.177(1900, 49152), 192.168.10.178(1900, 49152), 192.168.10.179(1900, 49152), 192.168.10.180(1900, 49152), 192.168.11.101(1900, 49152), 192.168.11.102(1900, 49152), 192.168.11.103(1900, 49152), 192.168.11.104(1900, 49152), 192.168.11.105(1900, 49152), 192.168.11.106(1900, 49152), 192.168.11.108(1900, 49152), 192.168.11.109(1900, 49152), 192.168.11.111(1900, 49152), 192.168.11.112(1900, 49152), 192.168.11.113(1900, 49152), 192.168.11.114(1900, 49152), 192.168.11.116(1900, 49152), 192.168.11.117(1900, 49152), 192.168.11.118(1900, 49152), 192.168.11.119(1900, 49152), 192.168.11.120(1900, 49152), 192.168.11.121(1900, 49152), 192.168.11.122(1900, 49152), 192.168.11.123(1900, 49152), 192.168.11.124(1900, 49152), 192.168.11.126(1900, 49152), 192.168.11.127(1900, 49152), 192.168.11.129(1900, 49152), 192.168.11.130(1900, 49152), 192.168.11.131(1900, 49152), 192.168.11.132(1900, 49152), 192.168.11.134(1900, 49152), 192.168.11.136(1900, 49152), 192.168.11.137(1900, 49152), 192.168.11.139(1900, 49152), 192.168.11.140(1900, 49152), 192.168.11.141(1900, 49152), 192.168.11.142(1900, 49152), 192.168.11.143(1900, 49152), 192.168.11.144(1900, 49152), 192.168.11.145(1900, 49152), 192.168.11.146(1900, 49152), 192.168.11.148(1900, 49152), 192.168.11.149(1900, 49152), 192.168.11.150(1900, 49152), 192.168.11.151(1900, 49152), 192.168.11.152(1900, 49152), 192.168.11.155(1900, 49152), 192.168.11.157(1900, 49152), 192.168.11.158(1900, 49152), 192.168.11.159(1900, 49152), 192.168.11.160(1900, 49152), 192.168.11.161(1900, 49152), 192.168.11.162(1900, 49152), 192.168.11.163(1900, 49152), 192.168.11.164(1900, 49152), 192.168.11.165(1900, 49152), 192.168.11.166(1900, 49152), 192.168.11.167(1900, 49152), 192.168.11.168(1900, 49152), 192.168.11.169(1900, 49152), 192.168.11.170(1900, 49152), 192.168.11.171(1900, 49152), 192.168.11.172(1900, 49152), 192.168.11.173(1900, 49152), 192.168.11.174(1900, 49152), 192.168.11.176(1900, 49152), 192.168.11.177(1900, 49152), 192.168.11.178(1900, 49152), 192.168.11.179(1900, 49152), 192.168.11.181(1900, 49152), 192.168.11.182(1900, 49152), 192.168.11.184(1900, 49152), 192.168.11.185(1900, 49152) | | |
| **Detail** | According to its banner, the version of MiniUPnP running on the remote host is prior to 1.4. It is, therefore, affected by the following vulnerabilities :   - An out-of-bounds read error exists in the  ProcessSSDPRequest() function in file minissdp.c that  allows an unauthenticated, remote attacker to cause a  denial of service condition via a specially crafted  M-SEARCH request. (CVE-2013-0229)   - A stack-based buffer overflow condition exists in the  ExecuteSoapAction() function in the SOAPAction handler,  due to improper validation of user-supplied input. An  unauthenticated, remote attacker can exploit this, via a  long quoted method, to cause a denial of service  condition or the execution of arbitrary code.  (CVE-2013-0230) | | |
| **Solution** | Upgrade to MiniUPnP version 1.4 or later. | | |
| **Remark** | http://www.nessus.org/u?46d66d2f https://help.rapid7.com/?community http://www.nessus.org/u?d381943f | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 10 | **Finding** | MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check) |
| **Severity** | Critical | **Port** | UDP: 5355 |
| **Target** | 192.168.11.9(5355), 192.168.11.189(5355) | | |
| **Detail** | A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.  Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely. | | |
| **Solution** | Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2. | | |
| **Remark** | https://www.nessus.org/u?361871b1 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 11 | **Finding** | Treck TCP/IP stack multiple vulnerabilities. (Ripple20) |
| **Severity** | Critical | **Port** | TCP: 0 |
| **Target** | 192.168.10.73(0) | | |
| **Detail** | This plugin detects the usage of the Treck TCP/IP stack by the host thereby indicating that it could be potentially vulnerable to the Ripple20 vulnerabilities. Patches are being slowly rolled out by vendors and we will release plugins for patches as they are released by the vendors. In the interim, if you have applied the patches from the vendor for the Ripple20 vulnerabilities on this host, please recast the severity of this plugin.  Note: This plugin requires ICMP traffic to be unblocked between the scanner and the host | | |
| **Solution** | Apply the relevant patches as they become available. | | |
| **Remark** | https://www.jsof-tech.com/ripple20/ http://www.nessus.org/u?431098c1 https://support.hp.com/emea\_africa-en/document/c06640149 https://psirt.bosch.com/security-advisories/BOSCH-SA-662084.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 12 | **Finding** | SSL Version 2 and 3 Protocol Detection |
| **Severity** | High | **Port** | TCP: 1433, 1480, 2381, 8082, 49160, 49208 |
| **Target** | 192.168.9.12(8082, 49208), 192.168.9.13(1480), 192.168.11.39(1433), 192.168.11.100(1480, 2381, 49160) | | |
| **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.** | 13 | **Finding** | HP System Management Homepage 7.2.0.14 iprange Parameter Code Execution |
| **Severity** | High | **Port** | TCP: 2381 |
| **Target** | 192.168.11.100(2381) | | |
| **Detail** | According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server is a version prior to 7.2.0.14 and is, therefore, reportedly affected by a code execution vulnerability related to the 'iprange' parameter in requests made to '/proxy/DataValidation'  Note that successful exploitation requires that anonymous access is enabled. | | |
| **Solution** | Upgrade to HP System Management Homepage 7.2.0.14 or later. | | |
| **Remark** | http://www.nessus.org/u?f2db75ce | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 14 | **Finding** | HP System Management Homepage 7.2.1.0 Multiple Vulnerabilities (BEAST) |
| **Severity** | High | **Port** | TCP: 2381 |
| **Target** | 192.168.11.100(2381) | | |
| **Detail** | According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server is a version prior to 7.2.1.0. It is, therefore, affected by the following vulnerabilities :   - An information disclosure vulnerability, known as BEAST,  exists in the SSL 3.0 and TLS 1.0 protocols due to a  flaw in the way the initialization vector (IV) is  selected when operating in cipher-block chaining (CBC)  modes. A man-in-the-middle attacker can exploit this  to obtain plaintext HTTP header data, by using a  blockwise chosen-boundary attack (BCBA) on an HTTPS  session, in conjunction with JavaScript code that uses  the HTML5 WebSocket API, the Java URLConnection API,  or the Silverlight WebClient API. (CVE-2011-3389)   - The utility 'apachectl' can receive a zero-length  directory name in the LD\_LIBRARY\_PATH via the 'envvars'  file. A local attacker with access to that utility  could exploit this to load a malicious Dynamic Shared  Object (DSO), leading to arbitrary code execution.  (CVE-2012-0883)   - Numerous, unspecified errors could allow remote denial  of service attacks. (CVE-2012-2110, CVE-2012-2329,  CVE-2012-2336, CVE-2013-2357, CVE-2013-2358,  CVE-2013-2359, CVE-2013-2360)   - The fix for CVE-2012-1823 does not completely correct  the CGI query parameter vulnerability. Disclosure of  PHP source code and code execution are still possible.  Note that this vulnerability is exploitable only when  PHP is used in CGI-based configurations. Apache with  'mod\_php' is not an exploitable configuration.  (CVE-2012-2311, CVE-2012-2335)   - Unspecified errors exist that could allow unauthorized  access. (CVE-2012-5217, CVE-2013-2355)   - Unspecified errors exist that could allow disclosure of  sensitive information. (CVE-2013-2356, CVE-2013-2363)   - An unspecified error exists that could allow cross-site  scripting attacks. (CVE-2013-2361)   - Unspecified errors exist that could allow a local  attacker to cause denial of service conditions.  (CVE-2013-2362, CVE-2013-2364)   - An as-yet unspecified vulnerability exists that could   cause a denial of service condition. (CVE-2013-4821) | | |
| **Solution** | Upgrade to HP System Management Homepage 7.2.1.0 or later. | | |
| **Remark** | https://www.zerodayinitiative.com/advisories/ZDI-13-204/ http://www.nessus.org/u?2031110c https://www.securityfocus.com/archive/1/528723/30/0/threaded https://www.imperialviolet.org/2011/09/23/chromeandbeast.html https://www.openssl.org/~bodo/tls-cbc.txt | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 15 | **Finding** | HP System Management Homepage ginkgosnmp.inc Command Injection |
| **Severity** | High | **Port** | TCP: 2381 |
| **Target** | 192.168.11.100(2381) | | |
| **Detail** | According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server is earlier than 7.2.2 and is, therefore, reportedly affected by a command injection vulnerability.  An input validation error exists in the file 'ginkgosnmp.inc' related to the last segment in a requested URL path. This input is later used in an 'exec' call and could allow an authenticated attacker to execute arbitrary commands. | | |
| **Solution** | Upgrade to HP System Management Homepage 7.2.2 or later. | | |
| **Remark** | http://www.nessus.org/u?3dbce491 https://www.securityfocus.com/archive/1/528713/30/0/threaded | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 16 | **Finding** | HP System Management Homepage 7.2.6 Multiple Vulnerabilities (FREAK) |
| **Severity** | High | **Port** | TCP: 2381 |
| **Target** | 192.168.11.100(2381) | | |
| **Detail** | According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server is prior to 7.2.6. It is, therefore, affected by multiple vulnerabilities, including remote code execution vulnerabilities, in several components and third-party libraries :   - HP SMH (XSRF)  - libcurl  - OpenSSL | | |
| **Solution** | Upgrade to HP System Management Homepage (SMH) version 7.2.6 or later. | | |
| **Remark** | http://www.nessus.org/u?5bc0a4e1 https://www.openssl.org/news/secadv/20150108.txt https://www.smacktls.com/#freak https://www.openssl.org/news/secadv/20150319.txt | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 17 | **Finding** | HP System Management Homepage 7.6 Multiple Vulnerabilities (HPSBMU03653) (httpoxy) |
| **Severity** | High | **Port** | TCP: 2381 |
| **Target** | 192.168.11.100(2381) | | |
| **Detail** | According to its banner, the version of HP System Management Homepage (SMH) hosted on the remote web server is prior to 7.6. It is, therefore, affected by the following vulnerabilities :   - A heap buffer overflow condition exists in OpenSSL in  the EVP\_EncodeUpdate() function within file  crypto/evp/encode.c that is triggered when handling  a large amount of input data. An unauthenticated, remote  attacker can exploit this to cause a denial of service  condition. (CVE-2016-2105)   - A heap buffer overflow condition exists in OpenSSL in  the EVP\_EncryptUpdate() function within file  crypto/evp/evp\_enc.c that is triggered when handling a  large amount of input data after a previous call occurs  to the same function with a partial block. An  unauthenticated, remote attacker can exploit this to  cause a denial of service condition. (CVE-2016-2106)   - Multiple flaws exist OpenSSL in the  aesni\_cbc\_hmac\_sha1\_cipher() function in file  crypto/evp/e\_aes\_cbc\_hmac\_sha1.c and the  aesni\_cbc\_hmac\_sha256\_cipher() function in file  crypto/evp/e\_aes\_cbc\_hmac\_sha256.c that are triggered  when the connection uses an AES-CBC cipher and AES-NI  is supported by the server. A man-in-the-middle attacker  can exploit these to conduct a padding oracle attack,  resulting in the ability to decrypt the network traffic.  (CVE-2016-2107)   - Multiple unspecified flaws exist in OpenSSL in the d2i  BIO functions when reading ASN.1 data from a BIO due to  invalid encoding causing a large allocation of memory.  An unauthenticated, remote attacker can exploit these to  cause a denial of service condition through resource  exhaustion. (CVE-2016-2109)   - A certificate validation bypass vulnerability exists in  cURL and libcurl due to improper validation of TLS  certificates. A man-in-the-middle attacker can exploit  this, via a spoofed certificate that appears valid, to  disclose or manipulate transmitted data. (CVE-2016-3739)   - An integer overflow condition exists in PHP in the  php\_raw\_url\_encode() function within file  ext/standard/url.c due to improper validation of  user-supplied input. An unauthenticated, remote attacker  can exploit this to have an unspecified impact.  (CVE-2016-4070)    - A flaw exists in PHP in the php\_snmp\_error() function  within file ext/snmp/snmp.c that is triggered when  handling format string specifiers. An unauthenticated,  remote attacker can exploit this, via a crafted SNMP  object, to cause a denial of service or to execute  arbitrary code. (CVE-2016-4071)   - An invalid memory write error exists in PHP when  handling the path of phar file names that allows an  attacker to have an unspecified impact. (CVE-2016-4072)   - A remote code execution vulnerability exists in PHP in  phar\_object.c due to improper handling of zero-length  uncompressed data. An unauthenticated, remote attacker  can exploit this, via a specially crafted TAR, ZIP, or  PHAR file, to cause a denial of service condition or the  execution of arbitrary code. (CVE-2016-4342)   - A remote code execution vulnerability exists in PHP in  the phar\_make\_dirstream() function within file  ext/phar/dirstream.c due to improper handling of  ././@LongLink files. An unauthenticated, remote attacker  can exploit this, via a specially crafted TAR file, to  cause a denial of service condition or the execution of  arbitrary code. (CVE-2016-4343)   - A cross-site scripting (XSS) vulnerability exists due to  improper validation of user-supplied input. An  unauthenticated, remote attacker can exploit this, via a  specially crafted request, to execute arbitrary script  code in a user's browser session. (CVE-2016-4393)   - An unspecified HTTP Strict Transport Security (HSTS)  bypass vulnerability exists that allows authenticated,  remote attackers to disclose sensitive information.  (CVE-2016-4394)   - A remote code execution vulnerability exists due to an  overflow condition in the mod\_smh\_config.so library  caused by improper validation of user-supplied input  when parsing the admin-group parameter supplied to the  /proxy/SetSMHData endpoint. An unauthenticated, remote  attacker can exploit this, via a specially crafted  request, to cause a denial of service condition or the  execution of arbitrary code. (CVE-2016-4395)   - A remote code execution vulnerability exists due to an  overflow condition in the mod\_smh\_config.so library  caused by improper validation of user-supplied input  when parsing the TKN parameter supplied to the  /Proxy/SSO endpoint. An unauthenticated, remote  attacker can exploit this, via a specially crafted  request, to cause a denial of service condition or the  execution of arbitrary code. (CVE-2016-4396)   - An out-of-bounds read error exists in PHP in the  php\_str2num() function in bcmath.c when handling  negative scales. An unauthenticated, remote attacker can  exploit this, via a crafted call, to cause a denial of  service condition or the disclosure of memory contents.  (CVE-2016-4537)   - A flaw exists in PHP the bcpowmod() function in bcmath.c  due to modifying certain data structures without  considering whether they are copies of the \_zero\_,  \_one\_, or \_two\_ global variables. An unauthenticated,  remote attacker can exploit this, via a crafted call, to  cause a denial of service condition. (CVE-2016-4538)   - A flaw exists in PHP in the xml\_parse\_into\_struct()  function in xml.c when handling specially crafted XML  contents. An unauthenticated, remote attacker can  exploit this to cause a denial of service condition.  (CVE-2016-4539)   - Multiple out-of-bounds read errors exist in PHP within  file ext/intl/grapheme/grapheme\_string.c when handling  negative offsets in the zif\_grapheme\_stripos() and  zif\_grapheme\_strpos() functions. An unauthenticated,  remote attacker can exploit these issues to cause a  denial of service condition or disclose memory contents.  (CVE-2016-4540, CVE-2016-4541)   - A flaw exists in PHP in the exif\_process\_IFD\_TAG()  function in exif.c due to improper construction of  spprintf arguments. An unauthenticated, remote attacker  can exploit this, via crafted header data, to cause an  out-of-bounds read error, resulting in a denial of  service condition or the disclosure of memory contents.  (CVE-2016-4542)   - A flaw exists in PHP in the exif\_process\_IFD\_in\_JPEG()  function in exif.c due to improper validation of IFD  sizes. An unauthenticated, remote attacker can exploit  this, via crafted header data, to cause an out-of-bounds  read error, resulting in a denial of service condition  or the disclosure of memory contents. (CVE-2016-4543)   - A man-in-the-middle vulnerability exists, known as  'httpoxy', in the Apache Tomcat, Apache HTTP Server, and  PHP components due to a failure to properly resolve  namespace conflicts in accordance with RFC 3875 section  4.1.18. The HTTP\_PROXY environment variable is set based  on untrusted user data in the 'Proxy' header of HTTP  requests. The HTTP\_PROXY environment variable is used by  some web client libraries to specify a remote proxy  server. A remote attacker can exploit this, via a  crafted 'Proxy' header in an HTTP request, to redirect  an application's internal HTTP traffic to an arbitrary  proxy server where it may be observed or manipulated.  (CVE-2016-5385, CVE-2016-5387, CVE-2016-5388)  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 HP System Management Homepage (SMH) version 7.6 or later. | | |
| **Remark** | http://www.nessus.org/u?b7e1b347 https://httpoxy.org https://www.tenable.com/security/research/tra-2016-32 https://www.zerodayinitiative.com/advisories/ZDI-16-587/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 18 | **Finding** | MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check) |
| **Severity** | High | **Port** | TCP: 445 |
| **Target** | 192.168.10.3(445), 192.168.11.6(445), 192.168.11.9(445), 192.168.11.39(445), 192.168.11.100(445), 192.168.11.189(445) | | |
| **Detail** | The remote Windows host is affected by the following vulnerabilities :   - Multiple remote code execution vulnerabilities exist in  Microsoft Server Message Block 1.0 (SMBv1) due to  improper handling of certain requests. An  unauthenticated, remote attacker can exploit these  vulnerabilities, via a specially crafted packet, to  execute arbitrary code. (CVE-2017-0143, CVE-2017-0144,  CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)   - An information disclosure vulnerability exists in  Microsoft Server Message Block 1.0 (SMBv1) due to  improper handling of certain requests. An  unauthenticated, remote attacker can exploit this, via a  specially crafted packet, to disclose sensitive  information. (CVE-2017-0147)  ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE. | | |
| **Solution** | Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.  For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices. | | |
| **Remark** | http://www.nessus.org/u?68fc8eff http://www.nessus.org/u?321523eb http://www.nessus.org/u?065561d0 http://www.nessus.org/u?d9f569cf https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/ http://www.nessus.org/u?b9d9ebf9 http://www.nessus.org/u?8dcab5e4 http://www.nessus.org/u?234f8ef8 http://www.nessus.org/u?4c7e0cf3 https://github.com/stamparm/EternalRocks/ http://www.nessus.org/u?59db5b5b | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 19 | **Finding** | SMB Server DOUBLEPULSAR Backdoor / Implant Detection (EternalRocks) |
| **Severity** | High | **Port** | TCP: 445 |
| **Target** | 192.168.11.6(445), 192.168.11.9(445), 192.168.11.100(445), 192.168.11.189(445) | | |
| **Detail** | Nessus detected the presence of DOUBLEPULSAR on the remote Windows host. DOUBLEPULSAR is one of multiple Equation Group SMB implants and backdoors disclosed on 2017/04/14 by a group known as the Shadow Brokers. The implant allows an unauthenticated, remote attacker to use SMB as a covert channel to exfiltrate data, launch remote commands, or execute arbitrary code.  EternalRocks is a worm that propagates by utilizing DOUBLEPULSAR. | | |
| **Solution** | Remove the DOUBLEPULSAR backdoor / implant and disable SMBv1. | | |
| **Remark** | http://www.nessus.org/u?43ec89df https://github.com/countercept/doublepulsar-detection-script https://github.com/stamparm/EternalRocks/ http://www.nessus.org/u?68fc8eff | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 20 | **Finding** | Microsoft Windows SMBv1 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 445 |
| **Target** | 192.168.11.6(445), 192.168.11.100(445) | | |
| **Detail** | The remote Windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled. It is, therefore, affected by multiple vulnerabilities :   - Multiple information disclosure vulnerabilities exist  in Microsoft Server Message Block 1.0 (SMBv1) due to  improper handling of SMBv1 packets. An unauthenticated,  remote attacker can exploit these vulnerabilities, via a  specially crafted SMBv1 packet, to disclose sensitive  information. (CVE-2017-0267, CVE-2017-0268,  CVE-2017-0270, CVE-2017-0271, CVE-2017-0274,  CVE-2017-0275, CVE-2017-0276)   - Multiple denial of service vulnerabilities exist in  Microsoft Server Message Block 1.0 (SMBv1) due to  improper handling of requests. An unauthenticated,  remote attacker can exploit these vulnerabilities, via a  specially crafted SMB request, to cause the system to  stop responding. (CVE-2017-0269, CVE-2017-0273,  CVE-2017-0280)   - Multiple remote code execution vulnerabilities exist in  Microsoft Server Message Block 1.0 (SMBv1) due to  improper handling of SMBv1 packets. An unauthenticated,  remote attacker can exploit these vulnerabilities, via a  specially crafted SMBv1 packet, to execute arbitrary  code. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278,  CVE-2017-0279)  Depending on the host's security policy configuration, this plugin cannot always correctly determine if the Windows host is vulnerable if the host is running a later Windows version (i.e., Windows 8.1, 10, 2012, 2012 R2, and 2016) specifically that named pipes and shares are allowed to be accessed remotely and anonymously. Tenable does not recommend this configuration, and the hosts should be checked locally for patches with one of the following plugins, depending on the Windows version : 100054, 100055, 100057, 100059, 100060, or 100061. | | |
| **Solution** | Apply the applicable security update for your Windows version :   - Windows Server 2008 : KB4018466  - Windows 7 : KB4019264  - Windows Server 2008 R2 : KB4019264  - Windows Server 2012 : KB4019216  - Windows 8.1 / RT 8.1. : KB4019215  - Windows Server 2012 R2 : KB4019215  - Windows 10 : KB4019474  - Windows 10 Version 1511 : KB4019473  - Windows 10 Version 1607 : KB4019472  - Windows 10 Version 1703 : KB4016871  - Windows Server 2016 : KB4019472 | | |
| **Remark** | http://www.nessus.org/u?c21268d4 http://www.nessus.org/u?b9253982 http://www.nessus.org/u?23802c83 http://www.nessus.org/u?8313bb60 http://www.nessus.org/u?7677c678 http://www.nessus.org/u?36da236c http://www.nessus.org/u?0981b934 http://www.nessus.org/u?c88efefa http://www.nessus.org/u?695bf5cc http://www.nessus.org/u?459a1e8c http://www.nessus.org/u?ea45bbc5 http://www.nessus.org/u?4195776a http://www.nessus.org/u?fbf092cf http://www.nessus.org/u?8c0cc566 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 21 | **Finding** | SNMP Agent Default Community Name (public) |
| **Severity** | High | **Port** | UDP: 161 |
| **Target** | 192.168.9.11(161), 192.168.10.76(161), 192.168.11.175(161) | | |
| **Detail** | It is possible to obtain the default community name of the remote SNMP server.  An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications). | | |
| **Solution** | Disable the SNMP service on the remote host if you do not use it. Either filter incoming UDP packets going to this port, or change the  default community string. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 22 | **Finding** | Hikvision IP Camera Remote Authentication Bypass |
| **Severity** | High | **Port** | TCP: 80 |
| **Target** | 192.168.11.175(80), 192.168.11.180(80), 192.168.11.183(80) | | |
| **Detail** | The remote Hikvision IP camera is affected by an authentication bypass vulnerability. A remote, unauthenticated attacker can read configurations (including account passwords), access the camera images, or modify the camera firmware. | | |
| **Solution** | Upgrade to a resolved firmware version as per the vendor advisory. | | |
| **Remark** | https://us.hikvision.com/en https://us.hikvision.com/en http://www.nessus.org/u?18ce5951 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 23 | **Finding** | Unsupported Web Server Detection |
| **Severity** | High | **Port** | TCP: 80 |
| **Target** | 192.168.11.6(80), 192.168.11.7(80) | | |
| **Detail** | According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.  Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities. | | |
| **Solution** | Remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 24 | **Finding** | Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness |
| **Severity** | Medium | **Port** | TCP: 3389 |
| **Target** | 192.168.11.7(3389), 192.168.11.100(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.** | 25 | **Finding** | SSL Certificate Signed Using Weak Hashing Algorithm |
| **Severity** | Medium | **Port** | TCP: 1433, 1480, 2381, 3389, 8082, 49160, 49208 |
| **Target** | 192.168.9.12(3389, 8082, 49208), 192.168.9.13(1480, 3389), 192.168.10.3(3389), 192.168.11.6(3389), 192.168.11.7(3389), 192.168.11.9(3389), 192.168.11.39(1433, 3389), 192.168.11.100(1480, 2381, 3389, 49160) | | |
| **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.** | 26 | **Finding** | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| **Severity** | Medium | **Port** | TCP: 1433, 1480, 2381, 3389, 8082, 49160, 49208 |
| **Target** | 192.168.9.12(3389, 8082, 49208), 192.168.9.13(1480, 3389), 192.168.10.3(3389), 192.168.11.6(3389), 192.168.11.7(3389), 192.168.11.9(3389), 192.168.11.39(1433, 3389), 192.168.11.100(1480, 2381, 3389, 49160) | | |
| **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.** | 27 | **Finding** | SSL Certificate with Wrong Hostname |
| **Severity** | Medium | **Port** | TCP: 1433, 1480, 7070, 49160 |
| **Target** | 192.168.9.13(1480), 192.168.11.7(7070), 192.168.11.39(1433), 192.168.11.100(1480, 49160) | | |
| **Detail** | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. | | |
| **Solution** | Purchase or generate a proper SSL certificate for this service. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 28 | **Finding** | SSL Certificate Cannot Be Trusted |
| **Severity** | Medium | **Port** | TCP: 443, 1433, 1480, 2381, 3389, 7070, 8082, 8443, 10000, 49160, 49208 |
| **Target** | 192.168.9.11(443, 10000), 192.168.9.12(3389, 8082, 49208), 192.168.9.13(1480, 3389), 192.168.10.3(3389), 192.168.10.75(443), 192.168.10.76(443), 192.168.11.6(3389), 192.168.11.7(3389, 7070), 192.168.11.9(3389), 192.168.11.39(1433, 3389), 192.168.11.100(1480, 2381, 3389, 49160), 192.168.11.133(443, 8443), 192.168.11.138(443, 8443), 192.168.11.154(443, 8443) | | |
| **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.** | 29 | **Finding** | SSL Self-Signed Certificate |
| **Severity** | Medium | **Port** | TCP: 443, 1433, 1480, 2381, 3389, 7070, 8082, 8443, 10000, 49160, 49208 |
| **Target** | 192.168.9.11(443, 10000), 192.168.9.12(3389, 8082, 49208), 192.168.9.13(1480, 3389), 192.168.10.3(3389), 192.168.10.75(443), 192.168.10.76(443), 192.168.11.6(3389), 192.168.11.7(3389, 7070), 192.168.11.9(3389), 192.168.11.39(1433, 3389), 192.168.11.100(1480, 2381, 3389, 49160), 192.168.11.133(443, 8443), 192.168.11.138(443, 8443), 192.168.11.154(443, 8443) | | |
| **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.** | 30 | **Finding** | SMB Signing not required |
| **Severity** | Medium | **Port** | TCP: 445 |
| **Target** | 192.168.9.13(445), 192.168.9.14(445), 192.168.10.3(445), 192.168.11.6(445), 192.168.11.7(445), 192.168.11.9(445), 192.168.11.39(445), 192.168.11.100(445), 192.168.11.189(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.** | 31 | **Finding** | Terminal Services Encryption Level is Medium or Low |
| **Severity** | Medium | **Port** | TCP: 3389 |
| **Target** | 192.168.11.7(3389), 192.168.11.100(3389) | | |
| **Detail** | The remote Terminal Services service is not configured to use strong cryptography.   Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes. | | |
| **Solution** | Change RDP encryption level to one of :   3. High   4. FIPS Compliant | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 32 | **Finding** | Terminal Services Doesn't Use Network Level Authentication (NLA) Only |
| **Severity** | Medium | **Port** | TCP: 3389 |
| **Target** | 192.168.11.7(3389), 192.168.11.100(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.** | 33 | **Finding** | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
| **Severity** | Medium | **Port** | TCP: 1433, 1480, 2381, 3389, 8082, 49160, 49208 |
| **Target** | 192.168.9.12(3389, 8082, 49208), 192.168.9.13(1480, 3389), 192.168.10.3(3389), 192.168.11.6(3389), 192.168.11.7(3389), 192.168.11.9(3389), 192.168.11.39(1433, 3389), 192.168.11.100(1480, 2381, 3389, 49160) | | |
| **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.** | 34 | **Finding** | HP System Management Homepage 7.3 Multiple Vulnerabilities |
| **Severity** | Medium | **Port** | TCP: 2381 |
| **Target** | 192.168.11.100(2381) | | |
| **Detail** | According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server may be affected by the following vulnerabilities :   - Versions prior to 7.3 are affected by an unspecified  information disclosure vulnerability. (CVE-2013-4846)   - Versions 7.1 through 7.2.2 are affected by an  unspecified cross-site request forgery vulnerability.  (CVE-2013-6188) | | |
| **Solution** | Upgrade to HP System Management Homepage 7.3 or later. | | |
| **Remark** | http://www.nessus.org/u?2d45fc52 https://www.securityfocus.com/archive/1/531406/30/0/threaded | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 35 | **Finding** | HP System Management Homepage 7.2.4.1 / 7.3.3.1 OpenSSL Multiple Vulnerabilities |
| **Severity** | Medium | **Port** | TCP: 2381 |
| **Target** | 192.168.11.100(2381) | | |
| **Detail** | According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server has an implementation of the OpenSSL library that is affected by the following vulnerabilities :   - An error exists in the ssl3\_read\_bytes() function that  allows data to be injected into other sessions. Note  that this issue is only exploitable if  'SSL\_MODE\_RELEASE\_BUFFERS' is enabled. (CVE-2010-5298)   - An error exists related to the implementation of the  Elliptic Curve Digital Signature Algorithm (ECDSA) that  allows nonce disclosure via the 'FLUSH+RELOAD' cache  side-channel attack. (CVE-2014-0076)   - A buffer overflow condition exists related to invalid  DTLS fragment handling that could lead to execution of  arbitrary code. Note this issue only affects OpenSSL  when used as a DTLS client or server. (CVE-2014-0195)   - An error exists in the do\_ssl3\_write() function that  allows a NULL pointer to be dereferenced, resulting in a  denial of service condition. Note that this issue is  exploitable only if 'SSL\_MODE\_RELEASE\_BUFFERS' is  enabled. (CVE-2014-0198)   - An error exists related to DTLS handshake handling that  could lead to denial of service attacks. Note that this  issue only affects OpenSSL when used as a DTLS client.  (CVE-2014-0221)   - An unspecified error exists that allows an attacker to  cause usage of weak keying material leading to  simplified man-in-the-middle attacks. (CVE-2014-0224)   - An unspecified error exists related to anonymous ECDH  ciphersuites that allows denial of service attacks. Note  that this issue only affects OpenSSL TLS clients.  (CVE-2014-3470) | | |
| **Solution** | Upgrade to HP System Management Homepage 7.2.4.1 (Windows 2003) / 7.3.3.1 (Linux or Windows) or later.  Note that version 7.3.3.1 for Linux x86 still contains OpenSSL v1.0.0d.  Ensure that any products with which such an install might communicate with have been updated to the latest versions to not be affected by the vulnerability covered by CVE-2014-0224. | | |
| **Remark** | http://www.nessus.org/u?f7990895 https://www.securityfocus.com/archive/1/532538/30/0/threaded https://www.securityfocus.com/archive/1/532642/30/0/threaded http://www.openssl.org/news/vulnerabilities.html#CVE-2010-5298 https://www.openssl.org/news/vulnerabilities.html#2014-0076 http://www.openssl.org/news/vulnerabilities.html#CVE-2014-0198 https://www.openssl.org/news/vulnerabilities.html#CVE-2014-0221 http://www.openssl.org/news/vulnerabilities.html#CVE-2014-0224 http://www.openssl.org/news/vulnerabilities.html#CVE-2014-3470 https://www.openssl.org/news/secadv/20140605.txt | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 36 | **Finding** | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |
| **Severity** | Medium | **Port** | TCP: 1433, 1480, 2381, 8082, 49160, 49208 |
| **Target** | 192.168.9.12(8082, 49208), 192.168.9.13(1480), 192.168.11.39(1433), 192.168.11.100(1480, 2381, 49160) | | |
| **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.** | 37 | **Finding** | HP System Management Homepage 7.2.5 / 7.4.1 Multiple Vulnerabilities (POODLE) |
| **Severity** | Medium | **Port** | TCP: 2381 |
| **Target** | 192.168.11.100(2381) | | |
| **Detail** | According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server is prior to 7.2.5 or 7.4.1. It is, therefore, affected by the following  vulnerabilities :   - An information disclosure vulnerability exists exists in  OpenSSL due to the pretty printing functions leaking  information from the stack. A remote attacker can  exploit this to disclose sensitive information that is  echoed from pretty printing output. (CVE-2014-3508)   - A race condition exists in OpenSSL that is triggered  when handling Elliptic Curve (EC) Point Format Extension  data in a resumed session. A remote attacker can exploit  this to corrupt memory, resulting in a denial of service  condition or the execution of arbitrary code.  (CVE-2014-3509)   - A flaw exists in OpenSSL related to handling fragmented  'ClientHello' messages that allows a man-in-the-middle  attacker to force usage of TLS 1.0 regardless of higher  protocol levels being supported by both the server and  the client. (CVE-2014-3511)   - A denial of service vulnerability exists in OpenSSL in  the DTLS SRTP extension parsing code due to improper  handling of handshake messages. A remote attacker can  exploit this, via a specially crafted handshake message,  to cause a memory leak, resulting in a denial of  service. (CVE-2014-3513)   - A man-in-the-middle (MitM) information disclosure  vulnerability, known as POODLE, exists due to the way  SSL 3.0 handles padding bytes when decrypting messages  encrypted using block ciphers in cipher block chaining  (CBC) mode. A MitM attacker 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.  (CVE-2014-3566)   - A denial of service vulnerability exists in OpenSSL due  to a failure to properly verify the integrity of session  tickets. A remote attacker can exploit this, via a large  number of invalid session tickets, to cause a memory  leak, resulting in a denial of service condition.  (CVE-2014-3567)   - An error exists in OpenSSL related to the build  configuration process and the 'no-ssl3' build option  that allows servers and clients to process insecure SSL  3.0 handshake messages. (CVE-2014-3568)   - A NULL pointer dereference flaw exists in OpenSSL that  is triggered when an SRP ciphersuite is specified  without being properly negotiated with the client. A  remote attacker controlling a malicious server can  exploit this to crash an OpenSSL client. (CVE-2014-3569)   - A remote code execution vulnerability exists due to a  buffer overflow condition in the Single Sign On (SSO)  module. A remote attacker, using a long parameter, can  exploit this to execute arbitrary code in the context of  SYSTEM. (CVE-2015-2133)  Note that these vulnerabilities only affect instances of SMH running on Windows and Linux hosts. | | |
| **Solution** | Upgrade to HP System Management Homepage (SMH) 7.2.5 / 7.4.1 or later. | | |
| **Remark** | http://www.nessus.org/u?8b982cec http://www.nessus.org/u?1f36637e https://www.zerodayinitiative.com/advisories/ZDI-15-262/ 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.** | 38 | **Finding** | MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) |
| **Severity** | Medium | **Port** | TCP: 1032, 49155 |
| **Target** | 192.168.11.6(49155), 192.168.11.39(1032), 192.168.11.100(49155), 192.168.11.189(49155) | | |
| **Detail** | The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database. | | |
| **Solution** | Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10. | | |
| **Remark** | http://www.nessus.org/u?52ade1e9 http://badlock.org/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 39 | **Finding** | HP System Management Homepage 7.6.1 Multiple Vulnerabilities (HPSBMU03753) |
| **Severity** | Medium | **Port** | TCP: 2381 |
| **Target** | 192.168.11.100(2381) | | |
| **Detail** | According to its banner, the version of HP System Management Homepage (SMH) hosted on the remote web server is prior to 7.6.1. It is, therefore, affected by multiple vulnerabilities including multiple local and remote code execution vulnerabilities.  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 HP System Management Homepage (SMH) version 7.6.1 or later. | | |
| **Remark** | http://www.nessus.org/u?05d894b4 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 40 | **Finding** | TLS Version 1.0 Protocol Detection |
| **Severity** | Medium | **Port** | TCP: 443, 1433, 1480, 2381, 3389, 8082, 49160, 49208 |
| **Target** | 192.168.9.12(3389, 8082, 49208), 192.168.9.13(1480, 3389), 192.168.10.3(3389), 192.168.10.76(443), 192.168.11.6(3389), 192.168.11.7(3389), 192.168.11.9(3389), 192.168.11.39(1433, 3389), 192.168.11.100(1480, 2381, 3389, 49160) | | |
| **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.** | 41 | **Finding** | JQuery 1.2 3.5.0 Multiple XSS |
| **Severity** | Medium | **Port** | TCP: 80, 8090 |
| **Target** | 192.168.11.6(80), 192.168.11.7(8090), 192.168.11.128(80), 192.168.11.153(80) | | |
| **Detail** | According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.  Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios  required for successful exploitation do not exist on devices running a PAN-OS release. | | |
| **Solution** | Upgrade to JQuery version 3.5.0 or later. | | |
| **Remark** | https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://security.paloaltonetworks.com/PAN-SA-2020-0007 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 42 | **Finding** | SSL Certificate Expiry |
| **Severity** | Medium | **Port** | TCP: 443, 8443 |
| **Target** | 192.168.10.75(443), 192.168.11.133(443, 8443) | | |
| **Detail** | This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired. | | |
| **Solution** | Purchase or generate a new SSL certificate to replace the existing one. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 43 | **Finding** | SNMP 'GETBULK' Reflection DDoS |
| **Severity** | Medium | **Port** | UDP: 161 |
| **Target** | 192.168.9.11(161), 192.168.10.76(161) | | |
| **Detail** | The remote SNMP daemon is responding with a large amount of data to a 'GETBULK' request with a larger than normal value for 'max-repetitions'. A remote attacker can use this SNMP server to conduct a reflected distributed denial of service attack on an arbitrary remote host. | | |
| **Solution** | Disable the SNMP service on the remote host if you do not use it. Otherwise, restrict and monitor access to this service, and consider changing the default 'public' community string. | | |
| **Remark** | http://www.nessus.org/u?8b551b5c http://www.nessus.org/u?bdb53cfc | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 44 | **Finding** | SSH Weak Algorithms Supported |
| **Severity** | Medium | **Port** | TCP: 22 |
| **Target** | 192.168.9.11(22) | | |
| **Detail** | Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys. | | |
| **Solution** | Contact the vendor or consult product documentation to remove the weak ciphers. | | |
| **Remark** | https://tools.ietf.org/html/rfc4253#section-6.3 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 45 | **Finding** | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) |
| **Severity** | Medium | **Port** | TCP: 8082 |
| **Target** | 192.168.9.12(8082) | | |
| **Detail** | The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key. | | |
| **Solution** | Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections. | | |
| **Remark** | https://drownattack.com/ https://drownattack.com/drown-attack-paper.pdf | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 46 | **Finding** | Modbus/TCP Coil Access |
| **Severity** | Medium | **Port** | TCP: 502 |
| **Target** | 192.168.10.54(502), 192.168.10.55(502), 192.168.10.56(502), 192.168.10.57(502), 192.168.10.58(502), 192.168.10.59(502), 192.168.10.60(502), 192.168.10.61(502), 192.168.10.62(502), 192.168.10.70(502), 192.168.10.71(502), 192.168.10.72(502), 192.168.10.74(502), 192.168.10.77(502) | | |
| **Detail** | Using function code 1, Modbus can reads the coils in a Modbus slave, which is commonly used by SCADA and DCS field devices. Coils refer to the binary output settings and are typically mapped to actuators. A sample of coil settings read from the device are provided by the plugin output.  The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a write coil message. | | |
| **Solution** | Restrict access to the Modbus port (TCP/502) to authorized Modbus clients. | | |
| **Remark** | http://www.modbus.org/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 47 | **Finding** | Modbus/TCP Discrete Input Access |
| **Severity** | Medium | **Port** | TCP: 502 |
| **Target** | 192.168.10.54(502), 192.168.10.55(502), 192.168.10.56(502), 192.168.10.58(502), 192.168.10.59(502), 192.168.10.60(502), 192.168.10.61(502), 192.168.10.62(502), 192.168.10.72(502) | | |
| **Detail** | Using function code 2, Modbus can read the discrete inputs from a Modbus slave, which is commonly used by SCADA and DCS field devices. Discrete inputs represent binary (i.e boolean) values that often map to switches, relays, or other sensors. A sample of discrete inputs read from the device are provided by the plugin output.  The ability to read discrete inputs may help an attacker profile a system. | | |
| **Solution** | Restrict access to the Modbus port (TCP/502) to authorized Modbus clients. | | |
| **Remark** | http://www.modbus.org | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 48 | **Finding** | Modbus/TCP Device Identification |
| **Severity** | Medium | **Port** | TCP: 502 |
| **Target** | 192.168.10.57(502), 192.168.10.71(502), 192.168.10.74(502), 192.168.10.77(502) | | |
| **Detail** | Nessus sent a Modbus Encapsulated Interface read request with MEI type 14 to obtain the device's Vendor Name, Product Code, and Major and Minor Revision. If supported, the data can include Vendor URL, Product Name, Model Name, and User Application Name. The alternative is to detect Modbus on valid error responses from a device not supporting the function code 43 and MEI 14. | | |
| **Solution** | Restrict access to the Modbus port (TCP/502) to authorized Modbus clients. | | |
| **Remark** | http://www.modbus.org/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 49 | **Finding** | Terminal Services Encryption Level is not FIPS-140 Compliant |
| **Severity** | Low | **Port** | TCP: 3389 |
| **Target** | 192.168.11.7(3389), 192.168.11.100(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.** | 50 | **Finding** | SSL Certificate Chain Contains RSA Keys Less Than 2048 bits |
| **Severity** | Low | **Port** | TCP: 1433, 8082, 49160, 49208 |
| **Target** | 192.168.9.12(8082, 49208), 192.168.11.39(1433), 192.168.11.100(49160) | | |
| **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.** | 51 | **Finding** | SSH Server CBC Mode Ciphers Enabled |
| **Severity** | Low | **Port** | TCP: 22 |
| **Target** | 192.168.9.11(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.** | 52 | **Finding** | SSH Weak MAC Algorithms Enabled |
| **Severity** | Low | **Port** | TCP: 22 |
| **Target** | 192.168.9.11(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.** | 53 | **Finding** | SSH Weak Key Exchange Algorithms Enabled |
| **Severity** | Low | **Port** | TCP: 22 |
| **Target** | 192.168.9.11(22), 192.168.10.76(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. |