**Vulnerability Assessment Report**

**For**



**Unix Cloud**

**Date March 03 2022**

**Document Security Level:** Confidential

**Document Version:** 1.0

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

|  |  |  |  |
| --- | --- | --- | --- |
| Unix Cloud | | INET Managed Services CO., LTD. | |
| Name |  | **Name** |  |
| Position |  | **Position** |  |
| Tel |  | **Tel** |  |
| Signature |  | **Signature** |  |

**Table of Contents**

[1. Restrictions on disclosure and use of information 4](#_Toc97201647)

[2. Operation Method 5](#_Toc97201648)

[3. Project Scope 6](#_Toc97201649)

[3.1 Infrastructure Vulnerability Assessment 6](#_Toc97201650)

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

[4. Testing Tools 7](#_Toc97201652)

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

[5.1 Target Information 8](#_Toc97201654)

[5.2 Executive summary 9](#_Toc97201655)

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

[5.2.2 Vulnerability by Target 9](#_Toc97201657)

[5.3 Infrastructure Vulnerability Detail 11](#_Toc97201658)

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

[6.1 Target Information 13](#_Toc97201660)

[6.2 Executive summary 14](#_Toc97201661)

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

[6.2.2 Vulnerability by Target 14](#_Toc97201663)

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

[7. Port Discovery 18](#_Toc97201665)

[8. Appendix 19](#_Toc97201666)

[8.1 About Nessus 19](#_Toc97201667)

[8.1.1 Nessus vulnerabilities 19](#_Toc97201668)

[8.1.2 Nessus risk score 19](#_Toc97201669)

[8.2 About Acunetix 21](#_Toc97201670)

[8.2.1 Acunetix web vulnerabilities 21](#_Toc97201671)

[8.2.2 Acunetix risk score 22](#_Toc97201672)

# Restrictions on disclosure and use of information

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

# Operation Method

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



Figure 1: Operation Method

# Project Scope

## **3.1 Infrastructure Vulnerability Assessment**

**Target / IP Address:**

| **No.** | **Domain / Server Name** | **Public IP Address** | **Private IP Address** | **OS/Model** | **Functions** | **Public Assessment** | **Private Assessment** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | DATABASE01 | - | 172.16.69.13 | Ubuntu 18 | Database Server 01 |  | ✓ |
| 2 | WEB01 | 123.123.123.123 | 172.16.69.14 | Ubuntu 20 | Web Server |  | ✓ |
| 3 | TERM | - | 172.16.69.52 | Windows Server 2016 | Terminal Server |  | ✓ |
| 4 | SMB01 | 12.12.12.12 | 172.16.69.53 | Windows Server 2019 | SMB Server |  | ✓ |
| 5 | DATABASE02 | - | 172.16.69.54 | Ubuntu 18 | Database Server 02 |  | ✓ |

## **3.2 Web Application Vulnerability Assessment**

**Target / IP Address:**

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

# Testing Tools

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

# Infrastructure Vulnerability Assessment

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

**Testing date:** March 30, 2021

**Tester IP Address:** 203.150.110.29

Diagram

Description automatically generated

Figure 2: Vulnerability Assessment from Public Access

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

**Testing date:** March 30, 2021

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

A picture containing diagram

Description automatically generated

Figure 3: Vulnerability Assessment from Private Access

## **5.1 Target Information**

| **No.** | **Domain / Server Name** | **IP Address** | **OS/Model** | **Port** |
| --- | --- | --- | --- | --- |
| 1 |  | 10.10.1.1 |  | TCP : 22, 443, 657, 2300, 2301, 5024 |
| 2 |  | 10.10.1.2 |  | TCP : 22, 443, 657, 2300, 2301, 5024 |
| 3 |  | 10.10.1.3 |  | TCP : 22, 111 UDP : 111, 161, 32778, 32779, 32780, 52357 |
| 4 |  | 10.10.1.4 |  | TCP : 22, 111 UDP : 111, 161, 32778, 32779, 32780, 52357 |
| 5 |  | 10.10.1.5 |  | TCP : 22, 111 UDP : 111, 161, 32768, 32785, 32786, 52357 |
| 6 |  | 10.10.1.6 |  | TCP : 22, 111 UDP : 111, 161, 32768, 32777, 32778, 52357 |
| 7 |  | 10.10.1.7 |  | TCP : 22, 80, 443, 1260, 3260, 5989, 8080, 8443 |
| 8 |  | 10.10.1.10 |  | TCP : 22, 80, 443, 1260, 3260, 5989, 8080, 8443 |
| 9 |  | 10.10.1.23 |  | TCP : 22, 2222, 7778 |
| 10 |  | 10.10.1.25 |  | TCP : 22, 2222, 7778 |
| 11 |  | 10.10.1.26 |  | TCP : 22, 1199, 1200, 1201, 1202, 1203, 4369, 5672, 8080, 8443 |
| 12 |  | 10.10.1.103 |  | TCP : 22 UDP : 161, 32770, 32772, 32774, 52357 |
| 13 |  | 10.10.1.104 |  | TCP : 22 UDP : 161, 32770, 32772, 32774, 52357 |
| 14 |  | 10.30.1.11 |  | TCP : 22, 80, 443, 2181, 3661, 8080, 8090, 9443, 9998, 10001, 27000, 50000 |
| 15 |  | 10.30.1.12 |  | TCP : 22, 111, 1918, 1920, 3661, 9999 UDP : 111 |
| 16 |  | 10.30.1.13 |  | TCP : 22, 80, 443 UDP : 5353 |
| 17 |  | 10.30.201.10 |  | TCP : 22, 37, 80, 111, 443, 2000, 2049, 4045, 5060, 5555, 8002, 8003, 8004, 8005, 9443, 11000 UDP : 111 |
| 18 |  | 10.30.201.12 |  | TCP : 2000, 5060 |
| 19 |  | 10.30.201.14 |  | TCP : 22, 111, 2000, 4045, 5060 |
| 20 |  | 10.30.201.16 |  | TCP : 22, 80, 111, 2000, 4045, 5060 |
| 21 |  | 10.40.1.13 |  | TCP : 22, 179, 657, 3100, 3306, 4001, 8001, 8080, 8443, 8500, 9099, 9100, 9443, 10252 UDP : 161 |
| 22 |  | 10.40.1.15 |  | TCP : 22, 80, 111, 139, 443, 445, 657, 873, 2049, 5000, 6200, 8080, 11211 UDP : 111 |
| 23 |  | 10.40.1.16 |  | TCP : 22, 111, 139, 445, 657, 873, 2049, 5000, 5431, 6200, 8080, 11211 UDP : 111 |
| 24 |  | 10.40.1.17 |  | TCP : 22, 111, 179, 9099, 9100 UDP : 111, 5353 |
| 25 |  | 10.40.1.18 |  | TCP : 22, 80, 443, 6443 UDP : 5353 |
| 26 |  | 172.16.1.1 |  | TCP : 21, 22, 23, 111, 657, 1334, 3192, 9090, 32770 UDP : 111 |
| 27 |  | 172.16.1.2 |  | TCP : 22, 80, 443, 5000, 8080, 9000, 9292 |
| 28 |  | 172.16.1.6 |  | TCP : 21, 22, 23, 111, 657, 1334, 3192, 32768 UDP : 111, 32770 |
| 29 |  | 172.16.1.7 |  | TCP : 21, 22, 23, 111, 657, 1334, 3192, 32768 UDP : 111, 32771 |
| 30 |  | 172.16.1.8 |  | TCP : 21, 22, 23, 111, 657, 1334, 3192, 32769, 32770 UDP : 111 |
| 31 |  | 172.16.1.11 |  | TCP : 21, 22, 23, 111, 657, 1334, 3192, 9090, 32770 UDP : 111, 500 |
| 32 |  | 172.16.1.12 |  | TCP : 22 |
| 33 |  | 172.16.1.121 |  | TCP : 21, 22, 23, 111, 657, 1334, 3192, 32769, 32773 UDP : 111, 32771, 32803 |
| 34 |  | 172.16.1.122 |  | TCP : 21, 22, 23, 111, 657, 1334, 3192, 32769, 32770 UDP : 111 |
| 35 |  | 172.16.150.11 |  | TCP : 21, 23, 111, 657, 1334, 3192, 32769, 32771 UDP : 111 |
| 36 |  | 172.16.150.12 |  | TCP : 21, 23, 111, 657, 1334, 3192, 32768, 32770 UDP : 111, 32770, 32783 |
| 37 |  | 172.16.150.21 |  | TCP : 21, 23, 111, 657, 1334, 3192, 32770, 32774 UDP : 111 |
| 38 |  | 172.16.150.22 |  | TCP : 21, 23, 111, 657, 1334, 3192, 32768, 32770 UDP : 111 |
| 39 |  | 172.16.150.90 |  | TCP : 22, 111, 6900, 8002, 8003, 10000, 34742 UDP : 111, 33857 |

## **5.2 Executive summary**

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

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

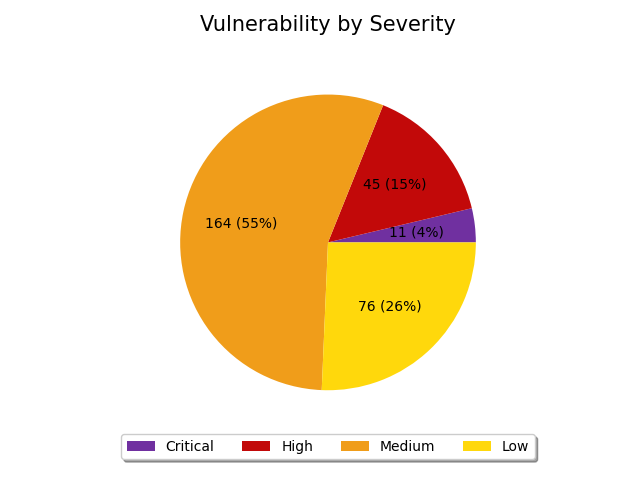


Figure 4: Summary by Severity of Infrastructure Vulnerability Assessment

### **5.2.2 Vulnerability by Target**

| **No.** | **Domain/Server Name** | **IP Address** | **Critical** | **High** | **Medium** | **Low** | **Total** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | - | 10.10.1.1 | 0 | 0 | 8 | 2 | 10 |
| 2 | - | 10.10.1.2 | 0 | 0 | 8 | 2 | 10 |
| 3 | - | 10.10.1.3 | 0 | 1 | 1 | 3 | 5 |
| 4 | - | 10.10.1.4 | 0 | 1 | 1 | 3 | 5 |
| 5 | - | 10.10.1.5 | 0 | 1 | 1 | 3 | 5 |
| 6 | - | 10.10.1.6 | 0 | 1 | 1 | 3 | 5 |
| 7 | - | 10.10.1.7 | 0 | 0 | 8 | 2 | 10 |
| 8 | - | 10.10.1.10 | 0 | 0 | 8 | 2 | 10 |
| 9 | - | 10.10.1.23 | 0 | 0 | 2 | 2 | 4 |
| 10 | - | 10.10.1.25 | 0 | 0 | 2 | 2 | 4 |
| 11 | - | 10.10.1.26 | 4 | 24 | 31 | 11 | 70 |
| 12 | - | 10.10.1.103 | 0 | 1 | 1 | 3 | 5 |
| 13 | - | 10.10.1.104 | 0 | 1 | 1 | 3 | 5 |
| 14 | - | 10.30.1.11 | 0 | 0 | 7 | 3 | 10 |
| 15 | - | 10.30.1.12 | 0 | 1 | 4 | 3 | 8 |
| 16 | - | 10.30.1.13 | 0 | 2 | 9 | 0 | 11 |
| 17 | - | 10.30.201.10 | 4 | 3 | 13 | 4 | 24 |
| 18 | - | 10.30.201.12 | 0 | 0 | 0 | 0 | 0 |
| 19 | - | 10.30.201.14 | 0 | 0 | 1 | 2 | 3 |
| 20 | - | 10.30.201.16 | 0 | 0 | 1 | 2 | 3 |
| 21 | - | 10.40.1.13 | 0 | 3 | 10 | 5 | 18 |
| 22 | - | 10.40.1.15 | 0 | 1 | 7 | 3 | 11 |
| 23 | - | 10.40.1.16 | 1 | 1 | 4 | 2 | 8 |
| 24 | - | 10.40.1.17 | 0 | 0 | 1 | 2 | 3 |
| 25 | - | 10.40.1.18 | 2 | 4 | 10 | 2 | 18 |
| 26 | - | 172.16.1.1 | 0 | 0 | 1 | 0 | 1 |
| 27 | - | 172.16.1.2 | 0 | 0 | 10 | 2 | 12 |
| 28 | - | 172.16.1.6 | 0 | 0 | 1 | 0 | 1 |
| 29 | - | 172.16.1.7 | 0 | 0 | 1 | 0 | 1 |
| 30 | - | 172.16.1.8 | 0 | 0 | 1 | 0 | 1 |
| 31 | - | 172.16.1.11 | 0 | 0 | 1 | 0 | 1 |
| 32 | - | 172.16.1.12 | 0 | 0 | 0 | 2 | 2 |
| 33 | - | 172.16.1.121 | 0 | 0 | 1 | 0 | 1 |
| 34 | - | 172.16.1.122 | 0 | 0 | 1 | 0 | 1 |
| 35 | - | 172.16.150.11 | 0 | 0 | 1 | 0 | 1 |
| 36 | - | 172.16.150.12 | 0 | 0 | 1 | 0 | 1 |
| 37 | - | 172.16.150.21 | 0 | 0 | 1 | 0 | 1 |
| 38 | - | 172.16.150.22 | 0 | 0 | 1 | 0 | 1 |
| 39 | - | 172.16.150.90 | 0 | 0 | 3 | 3 | 6 |
| **Total** | | | 11 | 45 | 164 | 76 | 296 |

## **5.3 Infrastructure Vulnerability Detail**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 1 | **Finding** | Python Unsupported Version Detection |
| **Severity** | Critical | **Port** | TCP: 6200 |
| **Target** | 10.40.1.16(6200) | | |
| **Detail** | The remote host contains one or more unsupported versions of Python. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. | | |
| **Solution** | Upgrade to a version of Python that is currently supported. | | |
| **Remark** | https://www.python.org/downloads/ https://devguide.python.org/devcycle/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 2 | **Finding** | nginx 0.6.x 1.20.1 1-Byte Memory Overwrite RCE |
| **Severity** | Critical | **Port** | TCP: 80, 443 |
| **Target** | 10.40.1.18(80, 443) | | |
| **Detail** | According to its Server response header, the installed version of nginx is 0.6.18 prior to 1.20.1. It is, therefore, affected by a remote code execution vulnerability. A security issue in nginx resolver was identified, which might allow an unauthenticated remote attacker to cause 1-byte memory overwrite by using a specially crafted DNS response, resulting in worker process crash or, potentially, in arbitrary code execution.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to nginx 1.20.1 or later. | | |
| **Remark** | http://mailman.nginx.org/pipermail/nginx-announce/2021/000300.html http://nginx.org/download/patch.2021.resolver.txt | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 3 | **Finding** | Unsupported Web Server Detection |
| **Severity** | Critical | **Port** | TCP: 5555 |
| **Target** | 10.30.201.10(5555) | | |
| **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.** | 4 | **Finding** | Apache 2.2.x 2.2.33-dev / 2.4.x 2.4.26 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 5555 |
| **Target** | 10.30.201.10(5555) | | |
| **Detail** | According to its banner, the version of Apache running on the remote host is 2.2.x prior to 2.2.33-dev or 2.4.x prior to 2.4.26. It is, therefore, affected by the following vulnerabilities :  - An authentication bypass vulnerability exists due to  third-party modules using the ap\_get\_basic\_auth\_pw()  function outside of the authentication phase. An  unauthenticated, remote attacker can exploit this to  bypass authentication requirements. (CVE-2017-3167)  - A NULL pointer dereference flaw exists due to  third-party module calls to the mod\_ssl  ap\_hook\_process\_connection() function during an HTTP  request to an HTTPS port. An unauthenticated, remote  attacker can exploit this to cause a denial of service  condition. (CVE-2017-3169)  - A NULL pointer dereference flaw exists in mod\_http2 that  is triggered when handling a specially crafted HTTP/2  request. An unauthenticated, remote attacker can exploit  this to cause a denial of service condition. Note that  this vulnerability does not affect 2.2.x.  (CVE-2017-7659)  - An out-of-bounds read error exists in the  ap\_find\_token() function due to improper handling of  header sequences. An unauthenticated, remote attacker  can exploit this, via a specially crafted header  sequence, to cause a denial of service condition.  (CVE-2017-7668)  - An out-of-bounds read error exists in mod\_mime due to  improper handling of Content-Type response headers. An  unauthenticated, remote attacker can exploit this, via a  specially crafted Content-Type response header, to cause  a denial of service condition or the disclosure of  sensitive information. (CVE-2017-7679) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache version 2.2.33-dev / 2.4.26 or later. | | |
| **Remark** | https://archive.apache.org/dist/httpd/CHANGES\_2.2.32 https://archive.apache.org/dist/httpd/CHANGES\_2.4.26 https://httpd.apache.org/security/vulnerabilities\_22.html https://httpd.apache.org/security/vulnerabilities\_24.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 5 | **Finding** | Apache 2.2.x 2.2.34 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 5555 |
| **Target** | 10.30.201.10(5555) | | |
| **Detail** | According to its banner, the version of Apache running on the remote host is 2.2.x prior to 2.2.34. It is, therefore, affected by the following vulnerabilities :  - An authentication bypass vulnerability exists in httpd  due to third-party modules using the  ap\_get\_basic\_auth\_pw() function outside of the  authentication phase. An unauthenticated, remote  attacker can exploit this to bypass authentication  requirements. (CVE-2017-3167)  - A denial of service vulnerability exists in httpd due to  a NULL pointer dereference flaw that is triggered when a  third-party module calls the mod\_ssl  ap\_hook\_process\_connection() function during an HTTP  request to an HTTPS port. An unauthenticated, remote  attacker can exploit this to cause a denial of service  condition. (CVE-2017-3169)  - A denial of service vulnerability exists in httpd due to  an out-of-bounds read error in the ap\_find\_token()  function that is triggered when handling a specially  crafted request header sequence. An unauthenticated,  remote attacker can exploit this to crash the  service or force ap\_find\_token() to return an incorrect  value. (CVE-2017-7668)  - A denial of service vulnerability exists in httpd due to  an out-of-bounds read error in the mod\_mime that is  triggered when handling a specially crafted Content-Type  response header. An unauthenticated, remote attacker can  exploit this to disclose sensitive information or cause  a denial of service condition. (CVE-2017-7679)  - A denial of service vulnerability exists in httpd due to  a failure to initialize or reset the value placeholder  in [Proxy-]Authorization headers of type 'Digest' before  or between successive key=value assignments by  mod\_auth\_digest. An unauthenticated, remote attacker can  exploit this, by providing an initial key with no '='  assignment, to disclose sensitive information or cause a  denial of service condition. (CVE-2017-9788) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache version 2.2.34 or later. | | |
| **Remark** | https://archive.apache.org/dist/httpd/CHANGES\_2.2.34 https://httpd.apache.org/security/vulnerabilities\_22.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 6 | **Finding** | Apache 2.4.49 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 5555 |
| **Target** | 10.30.201.10(5555) | | |
| **Detail** | The version of Apache httpd installed on the remote host is prior to 2.4.49. It is, therefore, affected by a vulnerability as referenced in the 2.4.49 changelog.  - A crafted request uri-path can cause mod\_proxy to forward the request to an origin server choosen by the  remote user. (CVE-2021-40438) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache version 2.4.49 or later. | | |
| **Remark** | https://downloads.apache.org/httpd/CHANGES\_2.4 https://httpd.apache.org/security/vulnerabilities\_24.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 7 | **Finding** | Apache 2.4.49 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 5555 |
| **Target** | 10.30.201.10(5555) | | |
| **Detail** | The version of Apache httpd installed on the remote host is prior to 2.4.49. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.49 changelog.  - ap\_escape\_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass  untrusted data to these functions, but third-party / external modules may. (CVE-2021-39275)  - Malformed requests may cause the server to dereference a NULL pointer. (CVE-2021-34798) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache version 2.4.49 or later. | | |
| **Remark** | https://downloads.apache.org/httpd/CHANGES\_2.4 https://httpd.apache.org/security/vulnerabilities\_24.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 8 | **Finding** | Apache Tomcat 8.5.0 8.5.32 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 8.5.x prior to 8.5.32. It is, therefore, affected by multiple vulnerabilities. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.32 or later. | | |
| **Remark** | http://www.nessus.org/u?5070a438 http://www.nessus.org/u?d5ab19d6 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 9 | **Finding** | Apache Tomcat 7.0.x 7.0.100 / 8.5.x 8.5.51 / 9.0.x 9.0.31 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Tomcat installed on the remote host is 7.0.x prior to 7.0.100, 8.x prior to 8.5.51, or 9.0.x prior to 9.0.31. It is, therefore, affected by multiple vulnerabilities.  - An HTTP request smuggling vulnerability exists in Tomcat due to mishandling Transfer-Encoding headers  behind a reverse proxy. An unauthenticated, remote attacker can exploit this, via crafted HTTP requests,  to cause unintended HTTP requests to reach the back-end. (CVE-2019-17569)  - An HTTP request smuggling vulnerability exists in Tomcat due to bad end-of-line (EOL) parsing that allowed  some invalid HTTP headers to be parsed as valid. An unauthenticated, remote attacker can exploit this, via  crafted HTTP requests, to cause unintended HTTP requests to reach the back-end. (CVE-2020-1935)  - An arbitrary file read vulnerability exists in Tomcat's Apache JServ Protocol (AJP) due to an  implementation defect. A remote, unauthenticated attacker could exploit this to access files which, under  normal conditions, would be restricted. If the Tomcat instance supports file uploads, the vulnerability  could also be leveraged to achieve remote code execution. (CVE-2020-1938) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version  number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.100, 8.5.51, 9.0.31 or later. | | |
| **Remark** | https://www.cnvd.org.cn/webinfo/show/5415 http://www.nessus.org/u?8ebe6246 http://www.nessus.org/u?4e287adb http://www.nessus.org/u?cbc3d54e | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 10 | **Finding** | SNMP Agent Default Community Name (public) |
| **Severity** | High | **Port** | UDP: 161 |
| **Target** | 10.10.1.3(161), 10.10.1.4(161), 10.10.1.5(161), 10.10.1.6(161), 10.10.1.103(161), 10.10.1.104(161), 10.40.1.13(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.** | 11 | **Finding** | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| **Severity** | High | **Port** | TCP: 443, 1200, 1201, 1202, 1203, 3661, 4001, 6443, 8001, 8002, 9443 |
| **Target** | 10.10.1.26(1200, 1201, 1202, 1203), 10.30.1.12(3661), 10.30.1.13(443), 10.30.201.10(443, 8002, 9443), 10.40.1.13(4001, 8001), 10.40.1.18(443, 6443) | | |
| **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.** | 12 | **Finding** | NFS Shares World Readable |
| **Severity** | High | **Port** | TCP: 2049 |
| **Target** | 10.40.1.15(2049), 10.40.1.16(2049) | | |
| **Detail** | The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range). | | |
| **Solution** | Place the appropriate restrictions on all NFS shares. | | |
| **Remark** | http://www.tldp.org/HOWTO/NFS-HOWTO/security.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 13 | **Finding** | nginx 1.9.5 1.16.1 / 1.17.x 1.17.3 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 80, 443 |
| **Target** | 10.40.1.18(80, 443) | | |
| **Detail** | According to its Server response header, the installed version of nginx is 1.9.5 prior to 1.16.1 or 1.17.x prior to 1.17.3. It is, therefore, affected by multiple denial of service vulnerabilities :   - A denial of service vulnerability exists in the HTTP/2 protocol stack due to improper handling of exceptional  conditions. An unauthenticated, remote attacker can exploit this, by manipulating the window size and stream  priority of a large data request, to cause a denial of service condition. (CVE-2019-9511)   - A denial of service vulnerability exists in the HTTP/2 protocol stack due to improper handling of exceptional  conditions. An unauthenticated, remote attacker can exploit this, by creating multiple request streams and  continually shuffling the priority of the streams, to cause a denial of service condition. (CVE-2019-9513)   - A denial of service vulnerability exists in the HTTP/2 protocol stack due to improper handling of exceptional  conditions. An unauthenticated, remote attacker can exploit this, by sending a stream of headers with a zero length  header name and zero length header value, to cause a denial of service condition. (CVE-2019-9516) | | |
| **Solution** | Upgrade to nginx version 1.16.1 / 1.17.3 or later. | | |
| **Remark** | http://www.nessus.org/u?b562be58 http://www.nessus.org/u?5ca4073f http://www.nessus.org/u?98fc786c | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 14 | **Finding** | Apache Tomcat 7.0.x 7.0.82 / 8.5.x 8.5.23 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 7.0.x prior to 7.0.82 or 8.5.x prior to 8.5.23. It is, therefore, affected by an unspecified vulnerability when running with HTTP PUTs enabled (e.g. via setting the readonly initialization parameter of the Default to false) that makes it possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server. Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.82 / 8.5.23 or later. | | |
| **Remark** | http://www.nessus.org/u?4f047e41 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 15 | **Finding** | Apache Tomcat 8.0.x 8.0.52 / 8.5.x 8.5.31 / 9.0.x 9.0.8 Denial of Service |
| **Severity** | High | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | According to its self-reported version number, the Apache Tomcat instance listening on the remote host is 8.0.x 8.0.52,  8.5.x 8.5.31 or 9.0.x 9.0.8. It is, therefore, affected  by the following vulnerability:  - A denial of service (DoS) vulnerability exists in   Tomcat due to improper overflow handling in the UTF-8  decoder. An unauthenticated, remote attacker can exploit   this issue to cause an infinite loop in the decoder,  leading to a denial of service condition. Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.0.52 / 8.5.31 / 9.0.8 or later. | | |
| **Remark** | http://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.0.52 http://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.5.31 http://tomcat.apache.org/security-9.html#Fixed\_in\_Apache\_Tomcat\_9.0.8 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 16 | **Finding** | Apache Tomcat 8.5.0 8.5.41 DoS |
| **Severity** | High | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.41. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_8.5.41\_security-8 advisory.  - The fix for CVE-2019-0199 was incomplete and did not  address HTTP/2 connection window exhaustion on write. By  not sending WINDOW\_UPDATE messages for the connection  window (stream 0) clients were able to cause server-side  threads to block eventually leading to thread exhaustion  and a DoS. (CVE-2019-10072) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.41 or later. | | |
| **Remark** | https://github.com/apache/tomcat/commit/0bcd69c https://github.com/apache/tomcat/commit/8d14c6f https://tomcat.apache.org/security-8.html#Fixed\_in\_Apache\_Tomcat\_8.5.41 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 17 | **Finding** | Apache Tomcat 8.5.0 8.5.49 Privilege Escalation |
| **Severity** | High | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.49. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_8.5.49\_security-8 advisory.  - When Apache Tomcat is configured with the JMX Remote   Lifecycle Listener, a local attacker without access to   the Tomcat process or configuration files is able to   manipulate the RMI registry to perform a man-in-the-middle   attack to capture user names and passwords used to access   the JMX interface. The attacker can then use these   credentials to access the JMX interface and gain complete   control over the Tomcat instance. (CVE-2019-12418) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.49 or later. | | |
| **Remark** | https://github.com/apache/tomcat/commit/a91d7db http://www.nessus.org/u?ed6582f2 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 18 | **Finding** | Apache Tomcat 8.5.0 8.5.50 Privilege Escalation Vulnerability |
| **Severity** | High | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.50. It is, therefore, affected by a privilege escalation vulnerability as referenced in the 'Fixed in Apache Tomcat 8.5.50' advisory.  - When using FORM authentication there was a narrow window where an attacker could perform a session  fixation attack. The window was considered too narrow for an exploit to be practical but, erring on the  side of caution, this issue has been treated as a security vulnerability. (CVE-2019-17563) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.50 or later. | | |
| **Remark** | https://github.com/apache/tomcat/commit/e19a202 http://www.nessus.org/u?e0b173ef | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 19 | **Finding** | Apache Tomcat 8.5.x 8.5.55 Remote Code Execution |
| **Severity** | High | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.x prior to 8.5.55. It is, therefore, affected by a  remote code execution vulnerability as referenced in the fixed\_in\_apache\_tomcat\_8.5.55\_security-8 advisory.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version  number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.55 or later. | | |
| **Remark** | http://www.nessus.org/u?9502c510 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 20 | **Finding** | Apache Tomcat 8.5.0 8.5.56 DoS |
| **Severity** | High | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.56. It is, therefore, affected by a denial of service vulnerability as referenced in the fixed\_in\_apache\_tomcat\_8.5.56\_security-8 advisory. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.56 or later. | | |
| **Remark** | http://www.nessus.org/u?9a501720 http://www.nessus.org/u?0ff2bf8c | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 21 | **Finding** | Apache Tomcat 8.5.0 8.5.57 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Tomcat installed on the remote host is 8.5.x prior to 8.5.57. It is, therefore, affected by multiple vulnerabilities as referenced in the Fixed in Apache Tomcat 8.5.57 security advisory.  - The payload length in a WebSocket frame was not correctly validated. Invalid payload lengths could trigger  an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service (DoS).  (CVE-2020-13935)  - An h2c direct connection did not release the HTTP/1.1 processor after the upgrade to HTTP/2. If a  sufficient number of such requests were made, an OutOfMemoryException could occur leading to a denial of  service (DoS). (CVE-2020-13934) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.57 or later. | | |
| **Remark** | http://www.nessus.org/u?cd59de72 http://www.nessus.org/u?7358785a http://www.nessus.org/u?78f0e4ba | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 22 | **Finding** | Apache Tomcat 8.5.x 8.5.60 Information Disclosure |
| **Severity** | High | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.60. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed\_in\_apache\_tomcat\_8.5.60\_security-8 advisory.  - When serving resources from a network location using the NTFS file system, Apache Tomcat versions  10.0.0-M1 to 10.0.0-M9, 9.0.0.M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP  source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE API  File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API  (FindFirstFileW) in some circumstances. (CVE-2021-24122)  - While investigating bug 64830 it was discovered that Apache Tomcat 10.0.0-M1 to 10.0.0-M9, 9.0.0-M1 to  9.0.39 and 8.5.0 to 8.5.59 could re-use an HTTP request header value from the previous stream received on  an HTTP/2 connection for the request associated with the subsequent stream. While this would most likely  lead to an error and the closure of the HTTP/2 connection, it is possible that information could leak  between requests. (CVE-2020-17527) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.60 or later. | | |
| **Remark** | http://www.nessus.org/u?05c4b1e2 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 23 | **Finding** | Apache Tomcat 8.5.0 8.5.63 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.63. It is, therefore, affected by multiple vulnerabilities as referenced in the vendor advisory.  - When responding to new h2c connection requests, Apache Tomcat versions 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41   and 8.5.0 to 8.5.61 could duplicate request headers and a limited amount of request body from one request to   another meaning user A and user B could both see the results of user A's request. (CVE-2021-25122)  - When using Apache Tomcat 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41, 8.5.0 to 8.5.61 or 7.0.0. to 7.0.107 with a   configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to   CVE-2020-9494. Note that both the previously published prerequisites for CVE-2020-9484 and the previously   published mitigations for CVE-2020-9484 also apply to this issue. (CVE-2021-25329) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.63 or later. | | |
| **Remark** | http://www.nessus.org/u?b6278e74 http://www.nessus.org/u?0be223a3 http://www.nessus.org/u?15b6baad | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 24 | **Finding** | SSL Version 2 and 3 Protocol Detection |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 10.30.1.13(443) | | |
| **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.** | 25 | **Finding** | SNMP 'GETBULK' Reflection DDoS |
| **Severity** | Medium | **Port** | UDP: 161 |
| **Target** | 10.10.1.3(161), 10.10.1.4(161), 10.10.1.5(161), 10.10.1.6(161), 10.10.1.103(161), 10.10.1.104(161), 10.40.1.13(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.** | 26 | **Finding** | SSL Certificate Cannot Be Trusted |
| **Severity** | Medium | **Port** | TCP: 443, 1200, 1201, 1202, 1203, 1260, 2301, 3661, 4001, 5000, 5024, 5989, 6443, 7778, 8001, 8002, 8003, 8080, 8443, 8500, 9000, 9292, 9443 |
| **Target** | 10.10.1.1(443, 2301, 5024), 10.10.1.2(443, 2301, 5024), 10.10.1.7(443, 1260, 5989, 8443), 10.10.1.10(443, 1260, 5989, 8443), 10.10.1.23(7778), 10.10.1.25(7778), 10.10.1.26(1200, 1201, 1202, 1203, 8443), 10.30.1.11(443, 9443), 10.30.1.12(3661), 10.30.1.13(443), 10.30.201.10(443, 8002, 9443), 10.40.1.13(4001, 8001, 8443, 8500, 9443), 10.40.1.15(443), 10.40.1.18(443, 6443), 172.16.1.2(443, 5000, 8080, 9000, 9292), 172.16.150.90(8003) | | |
| **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.** | 27 | **Finding** | SSL Self-Signed Certificate |
| **Severity** | Medium | **Port** | TCP: 443, 1200, 1201, 1202, 1203, 1260, 2301, 3661, 5000, 5024, 5989, 6443, 8002, 8003, 8080, 8443, 8500, 9000, 9292, 9443 |
| **Target** | 10.10.1.1(443, 2301, 5024), 10.10.1.2(443, 2301, 5024), 10.10.1.7(443, 1260, 5989, 8443), 10.10.1.10(443, 1260, 5989, 8443), 10.10.1.26(1200, 1201, 1202, 1203, 8443), 10.30.1.11(443, 9443), 10.30.1.12(3661), 10.30.1.13(443), 10.30.201.10(443, 8002, 9443), 10.40.1.13(8443, 8500), 10.40.1.15(443), 10.40.1.18(443, 6443), 172.16.1.2(443, 5000, 8080, 9000, 9292), 172.16.150.90(8003) | | |
| **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.** | 28 | **Finding** | TLS Version 1.0 Protocol Detection |
| **Severity** | Medium | **Port** | TCP: 443, 1200, 1201, 1202, 1203, 3661, 5024, 7778, 8002, 8500, 9443 |
| **Target** | 10.10.1.1(5024), 10.10.1.2(5024), 10.10.1.23(7778), 10.10.1.25(7778), 10.10.1.26(1200, 1201, 1202, 1203), 10.30.1.12(3661), 10.30.1.13(443), 10.30.201.10(443, 8002, 9443), 10.40.1.13(8500, 9443), 10.40.1.15(443), 10.40.1.18(443) | | |
| **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.** | 29 | **Finding** | HTTP TRACE / TRACK Methods Allowed |
| **Severity** | Medium | **Port** | TCP: 80, 443, 5000 |
| **Target** | 10.30.1.13(80, 443), 10.40.1.15(5000), 10.40.1.16(5000) | | |
| **Detail** | The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. | | |
| **Solution** | Disable these HTTP methods. Refer to the plugin output for more information. | | |
| **Remark** | https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper\_XST\_ebook.pdf http://www.apacheweek.com/issues/03-01-24 https://download.oracle.com/sunalerts/1000718.1.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 30 | **Finding** | Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials |
| **Severity** | Medium | **Port** | TCP: 445 |
| **Target** | 10.40.1.15(445), 10.40.1.16(445) | | |
| **Detail** | By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier), without credentials. The host SID can then be used to get the list of local users. | | |
| **Solution** | You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value. Refer to the 'See also' section for guidance. | | |
| **Remark** | http://technet.microsoft.com/en-us/library/bb418944.aspx | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 31 | **Finding** | SMB Use Host SID to Enumerate Local Users Without Credentials |
| **Severity** | Medium | **Port** | TCP: 445 |
| **Target** | 10.40.1.15(445), 10.40.1.16(445) | | |
| **Detail** | Using the host security identifier (SID), Nessus was able to enumerate local users on the remote Windows system, without credentials. | | |
| **Solution** | n/a | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 32 | **Finding** | SMB Signing not required |
| **Severity** | Medium | **Port** | TCP: 445 |
| **Target** | 10.40.1.15(445), 10.40.1.16(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.** | 33 | **Finding** | mDNS Detection (Remote Network) |
| **Severity** | Medium | **Port** | UDP: 5353 |
| **Target** | 10.30.1.13(5353), 10.40.1.17(5353), 10.40.1.18(5353) | | |
| **Detail** | The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.  This plugin attempts to discover mDNS used by hosts that are not on the network segment on which Nessus resides. | | |
| **Solution** | Filter incoming traffic to UDP port 5353, if desired. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 34 | **Finding** | nginx 1.x 1.14.1 / 1.15.x 1.15.6 Multiple Vulnerabilities |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 10.40.1.18(80, 443) | | |
| **Detail** | According to its Server response header, the installed version of nginx is 1.x prior to 1.14.1 or 1.15.x prior to 1.15.6. It is, therefore, affected by the following issues :   - An unspecified error exists related to the module  'ngx\_http\_v2\_module' that allows excessive memory usage.  (CVE-2018-16843)   - An unspecified error exists related to the module  'ngx\_http\_v2\_module' that allows excessive CPU usage.  (CVE-2018-16844)   - An unspecified error exists related to the module  'ngx\_http\_mp4\_module' that allows worker process  crashes or memory disclosure. (CVE-2018-16845) | | |
| **Solution** | Upgrade to nginx 1.14.1 / 1.15.6 or later. | | |
| **Remark** | http://nginx.org/en/security\_advisories.html http://mailman.nginx.org/pipermail/nginx-announce/2018/000220.html http://mailman.nginx.org/pipermail/nginx-announce/2018/000221.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 35 | **Finding** | nginx 1.17.7 Information Disclosure |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 10.40.1.18(80, 443) | | |
| **Detail** | According to its Server response header, the installed version of nginx is prior to 1.17.7. It is, therefore, affected by an information disclosure vulnerability. | | |
| **Solution** | Upgrade to nginx version 1.17.7 or later. | | |
| **Remark** | http://www.nessus.org/u?fd026623 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 36 | **Finding** | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
| **Severity** | Medium | **Port** | TCP: 443, 8002 |
| **Target** | 10.30.1.13(443), 10.30.201.10(8002) | | |
| **Detail** | The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext. | | |
| **Solution** | Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support. | | |
| **Remark** | https://www.rc4nomore.com/ http://www.nessus.org/u?ac7327a0 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ https://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 37 | **Finding** | Apache Server ETag Header Information Disclosure |
| **Severity** | Medium | **Port** | TCP: 5555 |
| **Target** | 10.30.201.10(5555) | | |
| **Detail** | The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files. | | |
| **Solution** | Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information. | | |
| **Remark** | http://httpd.apache.org/docs/2.2/mod/core.html#FileETag | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 38 | **Finding** | SSH Weak Algorithms Supported |
| **Severity** | Medium | **Port** | TCP: 22 |
| **Target** | 10.10.1.26(22), 10.30.1.11(22), 10.30.1.12(22), 10.30.201.10(22), 10.30.201.14(22), 10.30.201.16(22), 172.16.150.90(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.** | 39 | **Finding** | JQuery 1.2 3.5.0 Multiple XSS |
| **Severity** | Medium | **Port** | TCP: 5555 |
| **Target** | 10.30.201.10(5555) | | |
| **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.** | 40 | **Finding** | SSL Certificate Expiry |
| **Severity** | Medium | **Port** | TCP: 443, 1200, 1201, 1202, 1203, 5024, 8443, 9443 |
| **Target** | 10.10.1.1(5024), 10.10.1.2(5024), 10.10.1.26(1200, 1201, 1202, 1203, 8443), 10.30.1.11(9443), 10.30.1.13(443) | | |
| **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.** | 41 | **Finding** | Unencrypted Telnet Server |
| **Severity** | Medium | **Port** | TCP: 23 |
| **Target** | 172.16.1.1(23), 172.16.1.6(23), 172.16.1.7(23), 172.16.1.8(23), 172.16.1.11(23), 172.16.1.121(23), 172.16.1.122(23), 172.16.150.11(23), 172.16.150.12(23), 172.16.150.21(23), 172.16.150.22(23) | | |
| **Detail** | The remote host is running a Telnet server over an unencrypted channel.  Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a  remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.  SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session. | | |
| **Solution** | Disable the Telnet service and use SSH instead. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 42 | **Finding** | Apache Tomcat Default Files |
| **Severity** | Medium | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself. | | |
| **Solution** | Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to  replace or modify the default error page. | | |
| **Remark** | http://www.nessus.org/u?4cb3b4dd https://www.owasp.org/index.php/Securing\_tomcat | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 43 | **Finding** | AMQP Cleartext Authentication |
| **Severity** | Medium | **Port** | TCP: 5672 |
| **Target** | 10.10.1.26(5672) | | |
| **Detail** | The remote Advanced Message Queuing Protocol (AMQP) service supports one or more authentication mechanisms that allow credentials to be sent in the clear. | | |
| **Solution** | Disable cleartext authentication mechanisms in the AMQP configuration. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 44 | **Finding** | Apache Tomcat 8.5.x 8.5.34 Open Redirect Weakness |
| **Severity** | Medium | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 8.5.x prior to 8.5.34. It is, therefore, affected by a open redirect  vulnerability. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.34 or later. | | |
| **Remark** | http://www.nessus.org/u?1bddf0bb | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 45 | **Finding** | Apache Tomcat 8.5.x 8.5.58 / 9.0.x 9.0.38 HTTP/2 Request Mix-Up |
| **Severity** | Medium | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Tomcat installed on the remote host is 8.5.x prior to 8.5.58 or 9.0.x prior to 9.0.38. It is, therefore, affected by a vulnerability. If an HTTP/2 client exceeds the agreed maximum number of concurrent streams for a connection (in violation of the HTTP/2 protocol), it is possible that a subsequent request made on that connection could contain HTTP headers - including HTTP/2 pseudo headers - from a previous request rather than the intended headers. This can lead to users seeing responses for unexpected resources. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.58, 9.0.38 or later. | | |
| **Remark** | http://www.nessus.org/u?0656cf04 http://www.nessus.org/u?771617a1 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 46 | **Finding** | Apache Tomcat 7.0.x = 7.0.108 / 8.5.x = 8.5.65 / 9.0.x = 9.0.45 / 10.0.x = 10.0.5 vulnerability |
| **Severity** | Medium | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Tomcat installed on the remote host is 7.0.x = 7.0.108 / 8.5.x = 8.5.65 / 9.0.x = 9.0.45 / 10.0.x =  10.0.5. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_10.0.6\_security-10  advisory.  - Queries made by the JNDI Realm did not always correctly escape parameters. Parameter values could be  sourced from user provided data (eg user names) as well as configuration data provided by an  administrator. In limited circumstances it was possible for users to authenticate using variations of  their user name and/or to bypass some of the protection provided by the LockOut Realm. (CVE-2021-30640) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 7.0.109, 8.5.66, 9.0.46, 10.0.6 or later. | | |
| **Remark** | http://www.nessus.org/u?d3fb2d8e http://www.nessus.org/u?0fb6f5ab http://www.nessus.org/u?0d761c19 http://www.nessus.org/u?ddfa2b5e http://www.nessus.org/u?95156892 http://www.nessus.org/u?ed08487c http://www.nessus.org/u?806274b5 http://www.nessus.org/u?f104a57d https://bz.apache.org/bugzilla/show\_bug.cgi?id=65224 http://www.nessus.org/u?837a9443 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 47 | **Finding** | Apache Tomcat 8.5.0 8.5.68 vulnerability |
| **Severity** | Medium | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Tomcat installed on the remote host is prior to 8.5.68. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_8.5.68\_security-8 advisory.  - Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP  transfer-encoding request header in some circumstances leading to the possibility to request smuggling  when used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if  the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding;  and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.  (CVE-2021-33037) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.68 or later. | | |
| **Remark** | http://www.nessus.org/u?ca148f18 http://www.nessus.org/u?9e0e6b06 http://www.nessus.org/u?bea8fba1 http://www.nessus.org/u?836aea5f | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 48 | **Finding** | MongoDB 2.x, 3.0.x 3.0.15, 3.1.x 3.2.14, 3.3.x 3.3.14 Mongo Shell Information Disclosure Vulnerability (SERVER-25335) |
| **Severity** | Medium | **Port** | TCP: 27000 |
| **Target** | 10.30.1.11(27000) | | |
| **Detail** | The version of the remote MongoDB server is 2.x, 3.x 3.0.15, 3.2.x 3.2.14, 3.3.x 3.3.14. It is, therefore, affected by an information disclosure in mongo shell due to the MongoDB client having world-readable permissions on  .dbshell history files. An unauthenticated, local attacker can exploit this by reading these files to disclose  potentially sensitive information. 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 MongoDB version 3.0.15, 3.2.14, 3.3.14, 3.4 or later. | | |
| **Remark** | http://www.nessus.org/u?fabe3381 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 49 | **Finding** | OpenSSL AES-NI Padding Oracle MitM Information Disclosure |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 10.30.1.13(443) | | |
| **Detail** | The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability due to an error in the implementation of ciphersuites that use AES in CBC mode with HMAC-SHA1 or HMAC-SHA256. The implementation is specially written to use the AES acceleration available in x86/amd64 processors (AES-NI). The error messages returned by the server allow allow a man-in-the-middle attacker to conduct a padding oracle attack, resulting in the ability to decrypt network traffic. | | |
| **Solution** | Upgrade to OpenSSL version 1.0.1t / 1.0.2h or later. | | |
| **Remark** | https://blog.filippo.io/luckyminus20/ http://www.nessus.org/u?7647e9f0 https://www.openssl.org/news/secadv/20160503.txt | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 50 | **Finding** | SSH Server CBC Mode Ciphers Enabled |
| **Severity** | Low | **Port** | TCP: 22 |
| **Target** | 10.10.1.3(22), 10.10.1.4(22), 10.10.1.5(22), 10.10.1.6(22), 10.10.1.7(22), 10.10.1.10(22), 10.10.1.26(22), 10.10.1.103(22), 10.10.1.104(22), 10.30.1.11(22), 10.30.1.12(22), 10.40.1.13(22), 10.40.1.15(22), 10.40.1.16(22), 10.40.1.17(22), 10.40.1.18(22), 172.16.1.2(22), 172.16.1.12(22), 172.16.150.90(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.** | 51 | **Finding** | SSH Weak MAC Algorithms Enabled |
| **Severity** | Low | **Port** | TCP: 22 |
| **Target** | 10.10.1.3(22), 10.10.1.4(22), 10.10.1.5(22), 10.10.1.6(22), 10.10.1.26(22), 10.10.1.103(22), 10.10.1.104(22), 10.30.1.11(22), 10.30.1.12(22), 10.30.201.10(22), 10.30.201.14(22), 10.30.201.16(22), 172.16.150.90(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.** | 52 | **Finding** | SSH Weak Key Exchange Algorithms Enabled |
| **Severity** | Low | **Port** | TCP: 22, 2222 |
| **Target** | 10.10.1.1(22), 10.10.1.2(22), 10.10.1.3(22), 10.10.1.4(22), 10.10.1.5(22), 10.10.1.6(22), 10.10.1.7(22), 10.10.1.10(22), 10.10.1.23(22, 2222), 10.10.1.25(22, 2222), 10.10.1.26(22), 10.10.1.103(22), 10.10.1.104(22), 10.30.1.11(22), 10.30.1.12(22), 10.30.201.10(22), 10.30.201.14(22), 10.30.201.16(22), 10.40.1.13(22), 10.40.1.15(22), 10.40.1.16(22), 10.40.1.17(22), 10.40.1.18(22), 172.16.1.2(22), 172.16.1.12(22), 172.16.150.90(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 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 53 | **Finding** | Web Server HTTP Header Internal IP Disclosure |
| **Severity** | Low | **Port** | TCP: 8080, 8443 |
| **Target** | 10.40.1.13(8080, 8443) | | |
| **Detail** | This may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall or proxy server.  There is a known issue with Microsoft IIS 4.0 doing this in its default configuration. This may also affect other web servers, web applications, web proxies, load balancers and through a variety of misconfigurations related to redirection. | | |
| **Solution** | Apply configuration suggested by vendor. | | |
| **Remark** | http://www.nessus.org/u?fe24f941 https://support.microsoft.com/en-us/help/218180 http://www.nessus.org/u?4eedfe2d | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 54 | **Finding** | SSL/TLS Diffie-Hellman Modulus = 1024 Bits (Logjam) |
| **Severity** | Low | **Port** | TCP: 443, 1200, 1201, 1202, 1203, 5024, 9443 |
| **Target** | 10.10.1.1(5024), 10.10.1.2(5024), 10.10.1.26(1200, 1201, 1202, 1203), 10.30.201.10(443, 9443), 10.40.1.13(9443), 10.40.1.15(443) | | |
| **Detail** | The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections. | | |
| **Solution** | Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater. | | |
| **Remark** | https://weakdh.org/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 55 | **Finding** | Apache Tomcat 8.5.16 8.5.24 Insecure CGI Servlet Search Algorithm Description Weakness |
| **Severity** | Low | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 8.5.x prior to 8.5.24. It is, therefore, affected by a flaw that is due to  the program containing an incorrect description for the CGI Servlet search algorithm, which may cause an administrator to leave the  system in an insecure state. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.24 or later. | | |
| **Remark** | http://www.nessus.org/u?ffc49044 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 56 | **Finding** | Apache Tomcat 8.5.x 8.5.28 Security Constraint Weakness |
| **Severity** | Low | **Port** | TCP: 8080, 8443 |
| **Target** | 10.10.1.26(8080, 8443) | | |
| **Detail** | The version of Apache Tomcat installed on the remote host is 8.5.x prior to 8.5.28. It is, therefore, affected by a security constraints flaw which could expose resources to unauthorized users. | | |
| **Solution** | Upgrade to Apache Tomcat version 8.5.28 or later. | | |
| **Remark** | http://www.nessus.org/u?bebc5536 | | |



# 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. |