**รายงานสรุปผลการตรวจสอบช่องโหว่ของระบบ COCO-IDC3 All**

**บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) ประจำปี 2565**

# วัตถุประสงค์

1. เพื่อค้นหาจุดอ่อนและช่องโหว่บนระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของบริการ โดยใช้เทคนิคการตรวจสอบแบบ Vulnerability Assessment อ้างอิงจากมาตรฐาน Common Vulnerability Exposure, CVE และ Common Vulnerability Scoring System, CVSS-SIG
2. เพื่อนำเสนอข้อมูลจุดอ่อนหรือช่องโหว่ที่พบจากการตรวจสอบบนระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของบริการและเสนอแนะแนวทางในการแก้ไขจุดอ่อนและช่องโหว่ที่ตรวจพบ เพื่อให้ผู้ดูแลระบบเร่งดำเนินการแก้ไข

# เป้าหมาย

1. เพื่อให้ทราบถึงจุดอ่อนและช่องโหว่ของเครื่องที่ให้บริการ รวมถึงอุปกรณ์เครือข่ายภายในระบบสารสนเทศของบริการ
2. เพื่อนำเสนอข้อมูลจุดอ่อนหรือช่องโหว่ที่พบให้ ผู้ดูแลระบบ ผู้ดูแลเครือข่ายและผู้ดูแลระบบงานรับทราบถึงช่องโหว่ที่ตรวจพบเพื่อดำเนินการแก้ไข ปรับปรุงให้ระบบมีความแข็งแกร่งและยกระดับความมั่นคงปลอดภัยระบบสารสนเทศของบริการ

# แนวทางการประเมินความเสี่ยงที่พบ

การตรวจสอบจุดอ่อนและช่องโหว่ของเครื่องที่ให้บริการ และอุปกรณ์เครือข่ายภายในโครงสร้างระบบสารสนเทศ ดำเนินการตรวจสอบ โดยพิจารณาตามระดับความรุนแรงของจุดอ่อนและช่องโหว่ที่ตรวจพบ ซึ่งอ้างอิงตามมาตรฐาน Common Vulnerability Scoring System (CVSS) ที่ใช้เป็นมาตรฐานสากล โดยสามารถแบ่งระดับความรุนแรงของช่องโหว่ดังนี้

* **ความรุนแรงระดับวิกฤติ (CRITICAL)** หมายถึงจุดอ่อนหรือช่องโหว่ที่มีความเสี่ยงต่อการถูกบุกรุกระบบระดับวิกฤติ ผู้บุกรุกระบบสามารถใช้ช่องโหว่ที่ตรวจพบนี้โจมตีระบบได้ทันที และสร้างความเสียหายต่อระบบสารสนเทศในระดับวิกฤติ
* **ความรุนแรงระดับสูง (HIGH)** หมายถึงจุดอ่อนหรือช่องโหว่ที่มีความเสี่ยงต่อการถูกบุกรุกระบบระดับสูง ผู้บุกรุกระบบสามารถใช้ช่องโหว่ที่ตรวจพบนี้โจมตีระบบได้ทันที และสร้างความเสียหายต่อระบบสารสนเทศในระดับสูง
* **ความรุนแรงระดับกลาง (MEDIUM)** หมายถึงจุดอ่อนหรือช่องโหว่ที่มีความเสี่ยงต่อการถูกบุกรุกระบบระดับกลาง และผลกระทบของการบุกรุกระบบจะทำให้ระบบสารสนเทศมีความเสียหายในระดับกลาง
* **ความรุนแรงระดับต่ำ (LOW)** หมายถึงจุดอ่อนหรือช่องโหว่ที่มีความเสี่ยงต่อการถูกบุกรุกระบบระดับต่ำ และผลกระทบของการบุกรุกระบบทำให้ระบบสารสนเทศมีความเสียหายในระดับต่ำ
* **ไม่พบความรุนแรง (INFO)** หมายถึงรายละเอียดทั่วไปของระบบสารสนเทศ ซึ่งไม่มีผลกระทบต่อความเสียหายของระบบสารสนเทศ

**สารบัญ**

**หัวข้อ หน้า**

[วัตถุประสงค์ 1](#_Toc64730843)

[เป้าหมาย 1](#_Toc64730844)

[แนวทางการประเมินความเสี่ยงที่พบ 1](#_Toc64730845)

[ระยะเวลาในการดำเนินงาน 3](#_Toc64730846)

[รายงานสรุปผลการตรวจสอบ 3](#_Toc64730847)

[สรุปภาพโดยรวมช่องโหว่ที่ตรวจสอบพบบนระบบ Cloud Dell 4](#_Toc64730848)

[สรุปช่องโหว่พร้อมแนวทางแก้ไขโดยสังเขป 5](#_Toc64730849)

[ภาคผนวก รายละเอียดรายการ IP ที่ดำเนินการตรวจสอบช่องโหว่ 11](#_Toc64730850)

# ระยะเวลาในการดำเนินงาน

ดำเนินการตรวจสอบวิเคราะห์และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) ของระบบ COCO-IDC3 All จำนวน 516 รายการ ที่ บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) อาคารไทยซัมมิททาวเวอร์ ชั้น 10 ในวันที่ 02 มีนาคม 2565 เวลา 19:30 น. – 21:00 น.

# รายงานสรุปผลการตรวจสอบ

รายงานสรุปผลการตรวจสอบนี้ใช้สำหรับผู้ดูแลระบบ การเตรียมความพร้อมในการแก้ไขช่องโหว่ที่ตรวจพบมีจุดประสงค์เพื่อลดความรุนแรงและผลกระทบจากการถูกบุกรุกผ่านช่องโหว่ดังกล่าว จากผลการตรวจสอบสรุปจำนวนช่องโหว่ตามระดับความเสี่ยงจากภายในเครือข่ายของแต่ละเครื่อง/อุปกรณ์ดังตารางด้านล่างนี้

| รายการอุปกรณ์ | จำนวน IP | Critical | High | Medium | Low | Info |
| --- | --- | --- | --- | --- | --- | --- |
| Phase\_1 | 230 | 21 | 36 | 298 | 8 | 5991 |
| Phase\_2 | 158 | 236 | 14 | 164 | 7 | 3457 |
| Phase\_2.1 | 114 | 7 | 19 | 169 | 9 | 1708 |
| VM Server | 14 | 7 | 16 | 149 | 4 | 934 |
| Summary | 516 | 271 | 85 | 780 | 28 | 12090 |

**ตารางที่ 1** แสดงสรุปรายละเอียดผลการตรวจสอบช่องโหว่ที่ตรวจพบ

## สรุปภาพโดยรวมช่องโหว่ที่ตรวจสอบพบบนระบบ COCO-IDC3 All

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | สรุปภาพรวมในการตรวจสอบช่องโหว่บนระบบ COCO-IDC3 All  โดยมีเครื่องที่ให้บริการและอุปกรณ์เครือข่ายที่ได้รับการตรวจสอบ  ทั้งหมด จำนวน 516 รายการ   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **ระดับความรุนแรง** | **CRITICAL** | **HIGH** | **MED** | **LOW** | | **เปอร์เซ็นต์** | 23% | 7% | 67% | 2% | | **จำนวนช่องโหว่** | 271 | 85 | 780 | 28 | |

**ตารางที่ 2** แสดงภาพรวมช่องโหว่ที่ตรวจพบของระบบ Cloud Dell

## สรุปช่องโหว่พร้อมแนวทางแก้ไขโดยสังเขป

| ลำดับที่ | หมายเลขไอพี | รายละเอียดช่องโหว่ | ระดับความเสี่ยง | คำแนะนำในการแก้ไข |
| --- | --- | --- | --- | --- |
|  | 192.168.1.21 192.168.1.101 192.168.3.161 192.168.3.162 | Unsupported Windows OS (remote)  - 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. | **Critical** | * Upgrade to a supported service pack or operating system |
|  | 192.168.1.21 192.168.1.101 192.168.3.161 192.168.3.162 | Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)  - 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. | **Critical** | * Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2. |
|  | 192.168.1.11 192.168.2.81 192.168.2.82 192.168.2.83 192.168.2.84 192.168.2.85 192.168.2.87 192.168.2.88 192.168.2.89 192.168.2.90 192.168.2.91 192.168.2.92 192.168.2.93 192.168.2.94 192.168.2.95 192.168.2.96 192.168.2.97 192.168.2.98 192.168.2.99 192.168.2.104 192.168.2.105 192.168.2.106 192.168.2.107 192.168.2.108 192.168.2.109 192.168.2.110 192.168.2.111 192.168.2.112 192.168.2.113 192.168.2.114 192.168.2.115 192.168.2.116 192.168.2.117 192.168.2.118 192.168.2.119 192.168.2.120 192.168.2.121 192.168.2.122 192.168.2.123 192.168.2.124 192.168.2.125 192.168.2.126 192.168.2.127 192.168.2.128 192.168.2.129 192.168.2.130 192.168.2.132 192.168.2.133 192.168.2.134 192.168.2.135 192.168.2.136 192.168.2.137 192.168.2.138 192.168.2.139 192.168.2.140 192.168.2.141 192.168.2.142 192.168.2.143 192.168.2.144 192.168.2.145 192.168.2.146 192.168.2.148 192.168.2.149 192.168.2.150 192.168.2.151 192.168.2.152 192.168.2.153 192.168.2.154 192.168.2.156 192.168.2.157 192.168.2.158 192.168.2.159 192.168.2.160 192.168.2.161 192.168.2.162 192.168.2.163 192.168.2.164 192.168.2.165 192.168.2.166 192.168.2.167 192.168.2.168 192.168.2.169 192.168.2.170 192.168.2.171 192.168.2.172 192.168.2.173 192.168.2.174 192.168.2.175 192.168.2.176 192.168.2.177 192.168.2.179 192.168.2.180 192.168.2.181 192.168.2.184 192.168.2.186 192.168.2.187 192.168.2.188 192.168.2.189 192.168.2.190 192.168.2.191 192.168.2.192 192.168.2.193 192.168.2.194 192.168.2.196 192.168.2.198 192.168.2.200 192.168.2.202 192.168.2.205 192.168.2.206 192.168.2.207 192.168.2.210 192.168.2.212 192.168.2.213 192.168.2.214 192.168.2.215 192.168.2.216 192.168.2.218 192.168.2.219 192.168.2.220 192.168.2.222 192.168.2.223 192.168.2.224 192.168.2.225 192.168.2.226 192.168.2.227 | AXIS Multiple Vulnerabilities (ACV-128401)  - The firmware version running on the remote host is vulnerable to multiple vulnerabilities. An unauthenticated remote attacker could gain system-level unauthorized access to the affected device.  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | **Critical** | * Upgrade the host firmware to the version provided in the affected product list. |
|  | 192.168.1.21 192.168.3.161 192.168.13.19 | Web Server Directory Traversal Arbitrary File Access  - It appears possible to read arbitrary files on the remote host outside the web server's document directory using a specially crafted URL. An unauthenticated attacker may be able to exploit this issue to access sensitive information to aide in subsequent attacks. Note that this plugin is not limited to testing for known vulnerabilities in a specific set of web servers. Instead, it attempts a variety of generic directory traversal attacks and considers a product to be vulnerable simply if it finds evidence of the contents of '/etc/passwd' or a Windows 'win.ini' file in the response. It may, in fact, uncover 'new' issues, that have yet to be reported to the product's vendor. | **Critical** | * Contact the vendor for an update, use a different product, or disable the service altogether. |
|  | 192.168.1.24 192.168.1.26 192.168.1.27 192.168.1.28 192.168.1.30 192.168.1.51 192.168.1.52 192.168.1.53 192.168.1.54 192.168.1.55 192.168.1.56 192.168.1.57 | Treck TCP/IP stack multiple vulnerabilities. (Ripple20)  - 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 | **Critical** | * Apply the relevant patches as they become available. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.15 Multiple Vulnerabilities  - According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.15. It is, therefore, potentially affected by multiple vulnerabilities :  - A TLS renegotiation prefix injection attack is possible.   (CVE-2009-3555)  - The 'mod\_proxy\_ajp' module returns the wrong status code  if it encounters an error which causes the back-end   server to be put into an error state. (CVE-2010-0408)  - The 'mod\_isapi' attempts to unload the 'ISAPI.dll' when  it encounters various error states which could leave  call-backs in an undefined state. (CVE-2010-0425)  - A flaw in the core sub-request process code can lead to  sensitive information from a request being handled by   the wrong thread if a multi-threaded environment is  used. (CVE-2010-0434)  - Added 'mod\_reqtimeout' module to mitigate Slowloris  attacks. (CVE-2007-6750) | **Critical** | * Upgrade to Apache version 2.2.15 or later. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.13 APR apr\_palloc Heap Overflow  - According to its self-reported banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.13. As such, it includes a bundled version of the Apache Portable Runtime (APR) library that contains a flaw in 'apr\_palloc()' that could cause a heap overflow.  Note that the Apache HTTP server itself does not pass unsanitized, user-provided sizes to this function so it could only be triggered through some other application that uses it in a vulnerable way. | **Critical** | * Upgrade to Apache 2.2.13 or later. |
|  | 192.168.1.248 192.168.13.17 | PHP Unsupported Version Detection  - According to its version, the installation of PHP 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. | **Critical** | * Upgrade to a version of PHP that is currently supported. |
|  | 192.168.2.81 192.168.2.82 192.168.2.84 192.168.2.85 192.168.2.87 192.168.2.88 192.168.2.89 192.168.2.90 192.168.2.91 192.168.2.92 192.168.2.93 192.168.2.94 192.168.2.95 192.168.2.96 192.168.2.97 192.168.2.98 192.168.2.99 192.168.2.106 192.168.2.107 192.168.2.108 192.168.2.109 192.168.2.110 192.168.2.111 192.168.2.112 192.168.2.113 192.168.2.114 192.168.2.115 192.168.2.116 192.168.2.117 192.168.2.118 192.168.2.119 192.168.2.120 192.168.2.125 192.168.2.126 192.168.2.127 192.168.2.128 192.168.2.129 192.168.2.130 192.168.2.132 192.168.2.133 192.168.2.134 192.168.2.135 192.168.2.136 192.168.2.137 192.168.2.138 192.168.2.139 192.168.2.140 192.168.2.141 192.168.2.142 192.168.2.143 192.168.2.144 192.168.2.145 192.168.2.146 192.168.2.148 192.168.2.149 192.168.2.150 192.168.2.151 192.168.2.152 192.168.2.153 192.168.2.154 192.168.2.156 192.168.2.157 192.168.2.158 192.168.2.159 192.168.2.160 192.168.2.161 192.168.2.162 192.168.2.163 192.168.2.164 192.168.2.165 192.168.2.166 192.168.2.167 192.168.2.168 192.168.2.169 192.168.2.170 192.168.2.171 192.168.2.172 192.168.2.173 192.168.2.174 192.168.2.175 192.168.2.176 192.168.2.177 192.168.2.179 192.168.2.180 192.168.2.184 192.168.2.186 192.168.2.187 192.168.2.188 192.168.2.189 192.168.2.190 192.168.2.191 192.168.2.192 192.168.2.193 192.168.2.194 192.168.2.196 192.168.2.198 192.168.2.200 192.168.2.207 192.168.2.210 192.168.2.212 192.168.2.213 192.168.2.214 192.168.2.215 192.168.2.216 192.168.2.218 192.168.2.219 192.168.2.220 192.168.2.222 192.168.2.223 192.168.2.224 192.168.2.225 192.168.2.226 | AXIS HTTP GET Heap Overflow  - The remote AXIS device is affected by a heap overflow vulnerability in its web administration interface due to a flaw in handling of special characters. An unauthenticated remote attacker can exploit this vulnerability for denial of service and possibly remote code execution. | **Critical** | * Follow the vendor recommendation for upgrade or mitigation. |
|  | 192.168.3.128 192.168.3.130 | Dropbear SSH Server 2016.72 Multiple Vulnerabilities  - According to its self-reported version in its banner, Dropbear SSH running on the remote host is prior to 2016.74. It is, therefore, affected by the following vulnerabilities :  - A format string flaw exists due to improper handling of  string format specifiers (e.g., %s and %x) in usernames  and host arguments. An unauthenticated, remote attacker  can exploit this to execute arbitrary code with root  privileges. (CVE-2016-7406)  - A flaw exists in dropbearconvert due to improper  handling of specially crafted OpenSSH key files. An  unauthenticated, remote attacker can exploit this to  execute arbitrary code. (CVE-2016-7407)  - A flaw exists in dbclient when handling the -m or -c  arguments in scripts. An unauthenticated, remote attacker  can exploit this, via a specially crafted script, to  execute arbitrary code. (CVE-2016-7408)  - A flaw exists in dbclient or dropbear server if they are  compiled with the DEBUG\_TRACE option and then run using  the -v switch. A local attacker can exploit this to  disclose process memory. (CVE-2016-7409) | **Critical** | * Upgrade to Dropbear SSH version 2016.74 or later. |
|  | 192.168.13.11 192.168.13.22 192.168.13.23 | Microsoft SQL Server Unsupported Version Detection (remote check)  - 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. | **Critical** | * Upgrade to a version of Microsoft SQL Server that is currently supported. |
|  | 192.168.1.23 192.168.1.24 192.168.1.25 192.168.1.26 192.168.1.27 192.168.1.28 192.168.1.29 192.168.1.30 192.168.1.46 192.168.1.48 192.168.1.51 192.168.1.52 192.168.1.53 192.168.1.54 192.168.1.55 192.168.1.56 192.168.1.57 192.168.1.58 192.168.1.89 192.168.3.128 192.168.3.130 192.168.3.210 192.168.3.222 192.168.3.223 192.168.3.224 192.168.3.225 192.168.3.226 192.168.3.227 192.168.3.228 192.168.3.229 192.168.3.230 | SNMP Agent Default Community Name (public)  - 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). | **High** | * 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. |
|  | 192.168.1.248 192.168.13.17 | Unsupported Web Server Detection  - 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. | **High** | * Remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server. |
|  | 192.168.1.248 192.168.13.17 | PHP 5 5.2.7 Multiple Vulnerabilities  - According to its banner, the version of PHP installed on the remote host is prior to 5.2.7. It is, therefore, affected by multiple vulnerabilities :  - There is a buffer overflow flaw in the bundled PCRE  library that allows a denial of service attack.  (CVE-2008-2371)  - Multiple directory traversal vulnerabilities exist in  functions such as 'posix\_access', 'chdir', and 'ftok'  that allow a remote attacker to bypass 'safe\_mode'  restrictions. (CVE-2008-2665 and CVE-2008-2666).  - A buffer overflow flaw in 'php\_imap.c' may be triggered  when processing long message headers due to the use of  obsolete API calls. This can be exploited to cause a  denial of service or to execute arbitrary code.  (CVE-2008-2829)  - A buffer overflow in the 'imageloadfont' function in  'ext/gd/gd.c' can be triggered when a specially crafted  font is given. This can be exploited to cause a denial  of service or to execute arbitrary code. (CVE-2008-3658)  - A buffer overflow flaw exists in PHP's internal function  'memnstr' which can be exploited by an attacker using  the delimiter argument to the 'explode' function. This  can be used to cause a denial of service or to execute  arbitrary code. (CVE-2008-3659)  - When PHP is used as a FastCGI module, an attacker by  requesting a file whose file name extension is preceded  by multiple dots can cause a denial of service.  (CVE-2008-3660)  - A heap-based buffer overflow flaw in the mbstring  extension can be triggered via a specially crafted  string containing an HTML entity that is not handled  during Unicode conversion. This can be exploited to  execute arbitrary code.(CVE-2008-5557)  - Improper initialization of global variables 'page\_uid'  and 'page\_gid' when PHP is used as an Apache module  allows the bypassing of security restriction due to  SAPI 'php\_getuid' function overloading. (CVE-2008-5624)  - PHP does not enforce the correct restrictions when  'safe\_mode' is enabled through a 'php\_admin\_flag'  setting in 'httpd.conf'. This allows an attacker, by  placing a specially crafted 'php\_value' entry in  '.htaccess', to able to write to arbitrary files.  (CVE-2008-5625)  - The 'ZipArchive::extractTo' function in the ZipArchive  extension fails to filter directory traversal sequences  from file names. An attacker can exploit this to write  to arbitrary files. (CVE-2008-5658)  - Under limited circumstances, an attacker can cause a  file truncation to occur when calling the 'dba\_replace'  function with an invalid argument. (CVE-2008-7068)  - A buffer overflow error exists in the function  'date\_from\_ISO8601' function within file 'xmlrpc.c'  because user-supplied input is improperly validated.  This can be exploited by a remote attacker to cause a  denial of service or to execute arbitrary code.  (CVE-2014-8626) | **High** | * Upgrade to PHP version 5.2.8 or later. Note that version 5.2.7 has been removed from distribution because of a regression in that version that results in the 'magic\_quotes\_gpc' setting remaining off even if it was set to on. |
|  | 192.168.1.248 192.168.13.17 | PHP 5.2.8 Multiple Vulnerabilities  - According to its banner, the version of PHP installed on the remote host is earlier than 5.2.8. As such, it is potentially affected by the following vulnerabilities :  - PHP fails to properly sanitize error messages of  arbitrary HTML or script code, would code allow for   cross-site scripting attacks if PHP's 'display\_errors'   setting is enabled. (CVE-2008-5814)  - Version 5.2.7 introduced a regression with regard to  'magic\_quotes' functionality due to an incorrect fix to   the filter extension. As a result, the   'magic\_quotes\_gpc' setting remains off even if it is set   to on. (CVE-2008-5844) | **High** | * Upgrade to PHP version 5.2.8 or later. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.12 Multiple Vulnerabilities  - According to its banner, the version of Apache 2.2.x. running on the remote host is prior to 2.2.12. It is, therefore, affected by the following vulnerabilities :  - A heap-based buffer underwrite flaw exists in the  function 'apr\_strmatch\_precompile()' in the bundled copy  of the APR-util library, which could be triggered when  parsing configuration data to crash the daemon.  (CVE-2009-0023)  - A flaw in the mod\_proxy\_ajp module in version 2.2.11  only may allow a remote attacker to obtain sensitive  response data intended for a client that sent an  earlier POST request with no request body.  (CVE-2009-1191)  - The server does not limit the use of directives in a  .htaccess file as expected based on directives such  as 'AllowOverride' and 'Options' in the configuration  file, which could enable a local user to bypass  security restrictions. (CVE-2009-1195)  - Failure to properly handle an amount of streamed data  that exceeds the Content-Length value allows a remote  attacker to force a proxy process to consume CPU time  indefinitely when mod\_proxy is used in a reverse proxy  configuration. (CVE-2009-1890)  - Failure of mod\_deflate to stop compressing a file when  the associated network connection is closed may allow a  remote attacker to consume large amounts of CPU if  there is a large (>10 MB) file available that has  mod\_deflate enabled. (CVE-2009-1891)  - Using a specially crafted XML document with a large  number of nested entities, a remote attacker may be  able to consume an excessive amount of memory due to  a flaw in the bundled expat XML parser used by the  mod\_dav and mod\_dav\_svn modules. (CVE-2009-1955)  - There is an off-by-one overflow in the function  'apr\_brigade\_vprintf()' in the bundled copy of the  APR-util library in the way it handles a variable list  of arguments, which could be leveraged on big-endian  platforms to perform information disclosure or denial  of service attacks. (CVE-2009-1956) Note that Nessus has relied solely on the version in the Server response header and did not try to check for the issues themselves or even whether the affected modules are in use. | **High** | * Upgrade to Apache version 2.2.12 or later. Alternatively, ensure that the affected modules / directives are not in use. |
|  | 192.168.1.248 192.168.13.17 | PHP 5.2.11 Multiple Vulnerabilities  - According to its banner, the version of PHP installed on the remote host is older than 5.2.11. Such versions may be affected by several security issues :  - An unspecified error occurs in certificate validation  inside 'php\_openssl\_apply\_verification\_policy'.  - An unspecified input validation vulnerability affects  the color index in 'imagecolortransparent()'.  - An unspecified input validation vulnerability affects  exif processing.  - Calling 'popen()' with an invalid mode can cause a  crash under Windows. (Bug #44683)  - An integer overflow in 'xml\_utf8\_decode()' can make it  easier to bypass cross-site scripting and SQL injection   protection mechanisms using a specially crafted string   with a long UTF-8 encoding. (Bug #49687)  - 'proc\_open()' can bypass 'safe\_mode\_protected\_env\_vars'.  (Bug #49026) | **High** | * Upgrade to PHP version 5.2.11 or later. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.14 Multiple Vulnerabilities  - According to its banner, the version of Apache 2.2.x running on the  remote host is prior to 2.2.14. It is, therefore, potentially affected by multiple vulnerabilities :  - Faulty error handling in the Solaris pollset support   could lead to a denial of service. (CVE-2009-2699)  - The 'mod\_proxy\_ftp' module allows remote attackers to   bypass intended access restrictions. (CVE-2009-3095)  - The 'ap\_proxy\_ftp\_handler' function in   'modules/proxy/proxy\_ftp.c' in the 'mod\_proxy\_ftp'   module allows remote FTP servers to cause a   denial of service. (CVE-2009-3094) Note that the remote web server may not actually be affected by these vulnerabilities as Nessus did not try to determine whether the affected modules are in use or check for the issues themselves. | **High** | * Upgrade to Apache version 2.2.14 or later. Alternatively, ensure that the affected modules are not in use. |
|  | 192.168.1.248 192.168.13.17 | PHP 5.2 5.2.14 Multiple Vulnerabilities  - According to its banner, the version of PHP 5.2 installed on the remote host is older than 5.2.14. Such versions may be affected by several security issues :  - An error exists when processing invalid XML-RPC   requests that can lead to a NULL pointer  dereference. (bug #51288) (CVE-2010-0397)  - An error exists in the function 'fnmatch' that can lead  to stack exhaustion.  - An error exists in the sqlite extension that could   allow arbitrary memory access.  - A memory corruption error exists in the function  'substr\_replace'.  - The following functions are not properly protected  against function interruptions :  addcslashes, chunk\_split, html\_entity\_decode,   iconv\_mime\_decode, iconv\_substr, iconv\_mime\_encode,  htmlentities, htmlspecialchars, str\_getcsv,  http\_build\_query, strpbrk, strstr, str\_pad,  str\_word\_count, wordwrap, strtok, setcookie,   strip\_tags, trim, ltrim, rtrim, parse\_str, pack, unpack,   uasort, preg\_match, strrchr, strchr, substr, str\_repeat  (CVE-2010-1860, CVE-2010-1862, CVE-2010-1864,  CVE-2010-2097, CVE-2010-2100, CVE-2010-2101,  CVE-2010-2190, CVE-2010-2191, CVE-2010-2484)  - The following opcodes are not properly protected   against function interruptions :  ZEND\_CONCAT, ZEND\_ASSIGN\_CONCAT, ZEND\_FETCH\_RW  (CVE-2010-2191)  - The default session serializer contains an error  that can be exploited when assigning session  variables having user defined names. Arbitrary  serialized values can be injected into sessions by  including the PS\_UNDEF\_MARKER, '!', character in  variable names.  - A use-after-free error exists in the function  'spl\_object\_storage\_attach'. (CVE-2010-2225)  - An information disclosure vulnerability exists in the  function 'var\_export' when handling certain error   conditions. (CVE-2010-2531) | **High** | * Upgrade to PHP version 5.2.14 or later. |
|  | 192.168.1.248 192.168.13.17 | PHP 5.3.9 Multiple Vulnerabilities  - According to its banner, the version of PHP installed on the remote host is older than 5.3.9. As such, it may be affected by the following security issues :  - The 'is\_a()' function in PHP 5.3.7 and 5.3.8 triggers a   call to '\_\_autoload()'. (CVE-2011-3379)  - It is possible to create a denial of service condition   by sending multiple, specially crafted requests   containing parameter values that cause hash collisions   when computing the hash values for storage in a hash   table. (CVE-2011-4885)    - An integer overflow exists in the exif\_process\_IFD\_TAG   function in exif.c that can allow a remote attacker to   read arbitrary memory locations or cause a denial of   service condition. This vulnerability only affects PHP   5.4.0beta2 on 32-bit platforms. (CVE-2011-4566)  - Calls to libxslt are not restricted via  xsltSetSecurityPrefs(), which could allow an attacker  to create or overwrite files, resulting in arbitrary  code execution. (CVE-2012-0057)  - An error exists in the function 'tidy\_diagnose' that  can allow an attacker to cause the application to   dereference a NULL pointer. This causes the application  to crash. (CVE-2012-0781)  - The 'PDORow' implementation contains an error that can  cause application crashes when interacting with the   session feature. (CVE-2012-0788)  - An error exists in the timezone handling such that  repeated calls to the function 'strtotime' can allow  a denial of service attack via memory consumption.  (CVE-2012-0789) | **High** | * Upgrade to PHP version 5.3.9 or later. |
|  | 192.168.1.248 192.168.13.17 | PHP 5.3.12 / 5.4.2 CGI Query String Code Execution  - According to its banner, the version of PHP installed on the remote host is earlier than 5.3.12 / 5.4.2, and as such is potentially affected by a remote code execution and information disclosure vulnerability.  An error in the file 'sapi/cgi/cgi\_main.c' can allow a remote attacker to obtain PHP source code from the web server or to potentially execute arbitrary code. In vulnerable configurations, PHP treats certain query string parameters as command line arguments including switches such as '-s', '-d', and '-c'.  Note that this vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod\_php' is not an exploitable configuration. | **High** | * Upgrade to PHP version 5.3.12 / 5.4.2 or later. A 'mod\_rewrite' workaround is available as well. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.33-dev / 2.4.x 2.4.26 Multiple Vulnerabilities  - 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. | **High** | * Upgrade to Apache version 2.2.33-dev / 2.4.26 or later. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.34 Multiple Vulnerabilities  - 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. | **High** | * Upgrade to Apache version 2.2.34 or later. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.4.49 Multiple Vulnerabilities  - 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. | **High** | * Upgrade to Apache version 2.4.49 or later. |
|  | 192.168.1.60 192.168.3.80 | Wind River VxWorks 7.0 Multiple Vulnerabilities  - According to its self-reported version, the remote device is Wind River VxWorks and it's affected by multiple vulnerabilities:   - The memory allocator has a possible integer overflow in calculating a memory block's size to be allocated by  calloc(). As a result, the actual memory allocated is smaller than the buffer size specified by the arguments,  leading to memory corruption. (CVE-2020-35198)   - memory allocator has a possible overflow in calculating the memory block's size to be allocated by calloc().  As a result, the actual memory allocated is smaller than the buffer size specified by the arguments, leading  to memory corruption. (CVE-2020-13603)  Note that Nessus has not tested for this issue but has instead relied only on the OS version. | **High** | * Contact the device vendor to obtain the appropriate update |
|  | 192.168.1.60 192.168.3.80 | Wind River VxWorks = 6.8 RCE  - According to its self-reported version, the remote device is Wind River VxWorks and it's affected by a remote code execution vulnerability. An issue was discovered in Wind River VxWorks through 6.8. There is a possible stack overflow in dhcp server.  Note that Nessus has not tested for this issue but has instead relied only on the OS version. | **High** | * Contact the device vendor to obtain the appropriate update. |
|  | 192.168.1.62 192.168.1.63 192.168.1.68 192.168.13.11 192.168.13.20 192.168.13.22 192.168.13.23 | SSL Version 2 and 3 Protocol Detection  - 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'. | **High** | * Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead. |
|  | 192.168.2.86 192.168.2.131 192.168.2.147 192.168.2.178 192.168.2.195 192.168.2.211 192.168.2.221 192.168.2.228 | OpenSSL 1.1.1 1.1.1l Vulnerability  - The version of OpenSSL installed on the remote host is prior to 1.1.1l. It is, therefore, affected by a vulnerability as referenced in the 1.1.1l advisory.   - In order to decrypt SM2 encrypted data an application is expected to call the API function  EVP\_PKEY\_decrypt(). Typically an application will call this function twice. The first time, on entry, the  out parameter can be NULL and, on exit, the outlen parameter is populated with the buffer size  required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer  and call EVP\_PKEY\_decrypt() again, but this time passing a non-NULL value for the out parameter. A bug  in the implementation of the SM2 decryption code means that the calculation of the buffer size required to  hold the plaintext returned by the first call to EVP\_PKEY\_decrypt() can be smaller than the actual size  required by the second call. This can lead to a buffer overflow when EVP\_PKEY\_decrypt() is called by the  application a second time with a buffer that is too small. A malicious attacker who is able present SM2  content for decryption to an application could cause attacker chosen data to overflow the buffer by up to  a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing  application behaviour or causing the application to crash. The location of the buffer is application  dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).  (CVE-2021-3711)   - ASN.1 strings are represented internally within OpenSSL as an ASN1\_STRING structure which contains a  buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings  which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not  a strict requirement, ASN.1 strings that are parsed using OpenSSL's own d2i functions (and other similar  parsing functions) as well as any string whose value has been set with the ASN1\_STRING\_set() function will  additionally NUL terminate the byte array in the ASN1\_STRING structure. However, it is possible for  applications to directly construct valid ASN1\_STRING structures which do not NUL terminate the byte array  by directly setting the data and length fields in the ASN1\_STRING array. This can also happen by using  the ASN1\_STRING\_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to  assume that the ASN1\_STRING byte array will be NUL terminated, even though this is not guaranteed for  strings that have been directly constructed. Where an application requests an ASN.1 structure to be  printed, and where that ASN.1 structure contains ASN1\_STRINGs that have been directly constructed by the  application without NUL terminating the data field, then a read buffer overrun can occur. The same thing  can also occur during name constraints processing of certificates (for example if a certificate has been  directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the  certificate contains non NUL terminated ASN1\_STRING structures). It can also occur in the  X509\_get1\_email(), X509\_REQ\_get1\_email() and X509\_get1\_ocsp() functions. If a malicious actor can cause an  application to directly construct an ASN1\_STRING and then process it through one of the affected OpenSSL  functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack).  It could also result in the disclosure of private memory contents (such as private keys, or sensitive  plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected  1.0.2-1.0.2y). (CVE-2021-3712)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | **High** | * Upgrade to OpenSSL version 1.1.1l or later. |
|  | 192.168.3.161 192.168.3.162 | MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)  - 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. | **High** | * 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. |
|  | 192.168.3.161 192.168.3.162 | Microsoft Windows SMBv1 Multiple Vulnerabilities  - 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. | **High** | * 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 |
|  | 192.168.3.162 | SMB Server DOUBLEPULSAR Backdoor / Implant Detection (EternalRocks)  - 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. | **High** | * Remove the DOUBLEPULSAR backdoor / implant and disable SMBv1. |
|  | 192.168.1.2 192.168.1.3 192.168.1.4 192.168.1.5 192.168.1.6 192.168.1.7 192.168.1.8 192.168.1.9 192.168.1.10 192.168.1.12 192.168.1.13 192.168.1.21 192.168.1.76 192.168.1.77 192.168.1.78 192.168.1.79 192.168.1.80 192.168.1.83 192.168.1.84 192.168.1.85 192.168.1.86 192.168.1.87 192.168.1.88 192.168.1.89 192.168.1.102 192.168.1.104 192.168.1.105 192.168.1.106 192.168.1.107 192.168.1.108 192.168.1.110 192.168.1.111 192.168.1.112 192.168.1.113 192.168.1.115 192.168.1.116 192.168.1.117 192.168.1.119 192.168.1.120 192.168.1.121 192.168.1.122 192.168.1.123 192.168.1.124 192.168.1.125 192.168.1.126 192.168.1.127 192.168.1.128 192.168.1.129 192.168.1.133 192.168.1.136 192.168.1.137 192.168.1.139 192.168.1.141 192.168.1.142 192.168.1.143 192.168.1.144 192.168.1.145 192.168.1.146 192.168.1.147 192.168.1.148 192.168.1.149 192.168.1.150 192.168.1.151 192.168.1.152 192.168.1.161 192.168.1.162 192.168.1.163 192.168.1.164 192.168.1.167 192.168.1.168 192.168.1.169 192.168.1.170 192.168.1.171 192.168.1.172 192.168.1.173 192.168.1.174 192.168.1.175 192.168.1.176 192.168.1.177 192.168.1.178 192.168.1.179 192.168.1.180 192.168.1.181 192.168.1.182 192.168.1.183 192.168.1.184 192.168.1.185 192.168.1.186 192.168.1.187 192.168.1.188 192.168.1.189 192.168.1.190 192.168.1.191 192.168.1.192 192.168.1.193 192.168.1.194 192.168.1.195 192.168.1.196 192.168.1.197 192.168.1.198 192.168.1.199 192.168.1.200 192.168.1.201 192.168.1.202 192.168.1.203 192.168.1.204 192.168.1.205 192.168.1.206 192.168.1.207 192.168.1.208 192.168.1.209 192.168.1.211 192.168.1.212 192.168.1.213 192.168.1.214 192.168.1.215 192.168.1.216 192.168.1.224 192.168.1.225 192.168.1.226 192.168.1.227 192.168.1.228 192.168.1.229 192.168.1.230 192.168.1.231 192.168.1.232 192.168.1.233 192.168.1.234 192.168.1.235 192.168.1.236 192.168.1.237 192.168.1.238 192.168.1.239 192.168.1.240 192.168.1.241 192.168.1.242 192.168.1.243 192.168.1.244 192.168.1.245 192.168.1.246 192.168.1.247 192.168.3.128 192.168.3.130 192.168.3.161 192.168.3.210 192.168.3.222 192.168.3.223 192.168.3.224 192.168.3.225 192.168.3.227 192.168.3.228 192.168.3.229 192.168.3.230 | JQuery 1.2 3.5.0 Multiple XSS  - 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. | **Medium** | * Upgrade to JQuery version 3.5.0 or later. |
|  | 192.168.1.21 192.168.1.101 192.168.3.161 192.168.3.162 | Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness  - 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. | **Medium** | * - 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. |
|  | 192.168.1.21 192.168.1.62 192.168.1.63 192.168.1.68 192.168.1.101 192.168.3.161 192.168.3.162 192.168.13.11 192.168.13.20 192.168.13.22 192.168.13.23 | SSL Certificate Signed Using Weak Hashing Algorithm  - 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. | **Medium** | * Contact the Certificate Authority to have the SSL certificate reissued. |
|  | 192.168.1.21 192.168.1.61 192.168.1.62 192.168.1.63 192.168.1.68 192.168.1.101 192.168.1.248 192.168.1.254 192.168.3.161 192.168.3.162 192.168.3.163 192.168.3.231 192.168.3.232 192.168.13.11 192.168.13.12 192.168.13.14 192.168.13.16 192.168.13.17 192.168.13.18 192.168.13.19 192.168.13.20 192.168.13.21 192.168.13.22 192.168.13.23 192.168.13.24 | SSL Medium Strength Cipher Suites Supported (SWEET32)  - 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. | **Medium** | * Reconfigure the affected application if possible to avoid use of medium strength ciphers. |
|  | 192.168.1.11 192.168.1.21 192.168.1.61 192.168.1.62 192.168.1.63 192.168.1.68 192.168.1.101 192.168.1.248 192.168.1.254 192.168.2.86 192.168.2.131 192.168.2.147 192.168.2.195 192.168.2.217 192.168.2.221 192.168.2.228 192.168.3.60 192.168.3.161 192.168.3.162 192.168.3.163 192.168.3.220 192.168.3.231 192.168.3.232 192.168.13.11 192.168.13.12 192.168.13.14 192.168.13.16 192.168.13.17 192.168.13.18 192.168.13.19 192.168.13.20 192.168.13.21 192.168.13.22 192.168.13.23 192.168.13.24 | SSL Certificate Cannot Be Trusted  - 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. | **Medium** | * Purchase or generate a proper SSL certificate for this service. |
|  | 192.168.1.11 192.168.1.21 192.168.1.61 192.168.1.62 192.168.1.63 192.168.1.68 192.168.1.101 192.168.1.248 192.168.1.254 192.168.2.86 192.168.2.131 192.168.2.147 192.168.2.195 192.168.2.217 192.168.2.221 192.168.2.228 192.168.3.60 192.168.3.161 192.168.3.162 192.168.3.163 192.168.3.220 192.168.3.231 192.168.3.232 192.168.13.11 192.168.13.12 192.168.13.14 192.168.13.16 192.168.13.17 192.168.13.18 192.168.13.19 192.168.13.20 192.168.13.21 192.168.13.22 192.168.13.23 192.168.13.24 | SSL Self-Signed Certificate  - 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. | **Medium** | * Purchase or generate a proper SSL certificate for this service. |
|  | 192.168.1.15 192.168.1.21 192.168.1.61 192.168.1.101 192.168.3.162 192.168.3.163 192.168.13.11 192.168.13.12 192.168.13.14 192.168.13.16 192.168.13.17 192.168.13.18 192.168.13.19 192.168.13.20 192.168.13.21 192.168.13.22 192.168.13.23 192.168.13.24 | SMB Signing not required  - 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. | **Medium** | * 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. |
|  | 192.168.1.21 192.168.1.101 192.168.3.161 192.168.3.162 | Terminal Services Encryption Level is Medium or Low  - 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. | **Medium** | * Change RDP encryption level to one of :  3. High  4. FIPS Compliant |
|  | 192.168.1.21 192.168.1.101 192.168.3.161 192.168.3.162 | Terminal Services Doesn't Use Network Level Authentication (NLA) Only  - 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. | **Medium** | * Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows. |
|  | 192.168.1.21 192.168.1.62 192.168.1.63 192.168.1.68 192.168.1.101 192.168.3.161 192.168.3.162 192.168.3.163 192.168.13.11 192.168.13.12 192.168.13.14 192.168.13.16 192.168.13.17 192.168.13.18 192.168.13.19 192.168.13.20 192.168.13.21 192.168.13.22 192.168.13.23 192.168.13.24 | SSL RC4 Cipher Suites Supported (Bar Mitzvah)  - 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. | **Medium** | * 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. |
|  | 192.168.1.11 192.168.1.21 192.168.1.61 192.168.1.62 192.168.1.63 192.168.1.68 192.168.1.101 192.168.1.248 192.168.2.217 192.168.3.161 192.168.3.162 192.168.3.163 192.168.13.11 192.168.13.12 192.168.13.14 192.168.13.16 192.168.13.17 192.168.13.18 192.168.13.19 192.168.13.20 192.168.13.21 192.168.13.22 192.168.13.23 192.168.13.24 | TLS Version 1.0 Protocol Detection  - 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. | **Medium** | * Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0. |
|  | 192.168.1.11 192.168.2.86 192.168.2.131 192.168.2.147 192.168.2.178 192.168.2.195 192.168.2.211 192.168.2.217 192.168.2.221 192.168.2.227 192.168.2.228 | AXIS OS 5.51 5.51.7.5 / 6.0 6.50.5.5 / 7.0 8.40.4.3 / 9.0 9.80.3.5 / 10.0 10.8 Multiple Vulnerabilities  - The firmware version running on the remote host is vulnerable to multiple vulnerabilities, including the following:   - User controlled parameters related to SMTP notifications are not correctly validated. This can lead to a  buffer overflow resulting in crashes and data leakage. (CVE-2021-31986)   - A user controlled parameter related to SMTP test functionality is not correctly validated making it  possible to bypass blocked network recipients. (CVE-2021-31987)   - A user controlled parameter related to SMTP test functionality is not correctly validated making it  possible to add the Carriage Return and Line Feed (CRLF) control characters and include arbitrary SMTP  headers in the generated test email. (CVE-2021-31988)   Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | **Medium** | * Upgrade the host firmware.. |
|  | 192.168.1.21 192.168.13.11 192.168.13.12 192.168.13.17 192.168.13.20 192.168.13.21 192.168.13.22 192.168.13.23 | SSL Certificate with Wrong Hostname  - The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. | **Medium** | * Purchase or generate a proper SSL certificate for this service. |
|  | 192.168.1.23 192.168.1.24 192.168.1.25 192.168.1.26 192.168.1.27 192.168.1.28 192.168.1.29 192.168.1.30 192.168.1.51 192.168.1.52 192.168.1.53 192.168.1.54 192.168.1.55 192.168.1.56 192.168.1.57 192.168.1.58 192.168.3.22 192.168.3.23 192.168.3.25 192.168.3.26 192.168.3.27 192.168.3.28 192.168.3.29 192.168.3.30 192.168.3.31 192.168.3.32 192.168.3.33 192.168.3.34 192.168.3.35 192.168.3.36 192.168.3.37 192.168.3.38 192.168.3.39 192.168.3.40 192.168.3.41 192.168.3.42 192.168.3.43 192.168.3.44 192.168.3.45 192.168.3.46 192.168.3.47 192.168.3.48 192.168.3.49 192.168.3.50 192.168.3.51 192.168.3.52 192.168.3.53 192.168.3.55 192.168.3.56 192.168.3.57 192.168.3.58 192.168.3.59 192.168.3.60 192.168.3.61 192.168.3.62 192.168.3.63 192.168.3.64 192.168.3.65 192.168.3.66 192.168.3.67 192.168.3.68 192.168.3.69 192.168.3.70 192.168.3.71 192.168.3.72 192.168.3.73 192.168.3.74 192.168.3.75 192.168.3.127 192.168.3.128 192.168.3.129 192.168.3.130 192.168.3.131 192.168.3.132 192.168.3.133 192.168.3.134 192.168.3.220 | IP Forwarding Enabled  - The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.  Unless the remote host is a router, it is recommended that you disable IP forwarding. | **Medium** | * On Linux, you can disable IP forwarding by doing :  echo 0 > /proc/sys/net/ipv4/ip\_forward  On Windows, set the key 'IPEnableRouter' to 0 under  HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters  On Mac OS X, you can disable IP forwarding by executing the command :  sysctl -w net.inet.ip.forwarding=0  For other systems, check with your vendor. |
|  | 192.168.1.23 192.168.1.26 192.168.1.27 192.168.1.28 192.168.1.29 192.168.1.51 192.168.1.54 192.168.1.56 192.168.1.57 192.168.1.58 192.168.1.89 192.168.3.128 192.168.3.130 192.168.3.210 192.168.3.222 192.168.3.223 192.168.3.224 192.168.3.225 192.168.3.226 192.168.3.227 192.168.3.228 192.168.3.229 192.168.3.230 | SNMP 'GETBULK' Reflection DDoS  - 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. | **Medium** | * 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. |
|  | 192.168.1.248 192.168.13.17 | HTTP TRACE / TRACK Methods Allowed  - 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. | **Medium** | * Disable these HTTP methods. Refer to the plugin output for more information. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.9 Multiple Vulnerabilities (DoS, XSS)  - According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.9. It is, therefore, affected by multiple vulnerabilities :  - Improper handling of excessive forwarded interim   responses may cause denial of service conditions in   mod\_proxy\_http. (CVE-2008-2364)  - A cross-site request forgery vulnerability in the   balancer-manager interface of mod\_proxy\_balancer.  (CVE-2007-6420) Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves. | **Medium** | * Upgrade to Apache version 2.2.9 or later. Alternatively, ensure that the affected modules are not in use. |
|  | 192.168.1.248 192.168.13.17 | PHP 5.2.9 Multiple Vulnerabilities  - According to its banner, the version of PHP installed on the remote host is older than 5.2.9. Such versions may be affected by several security issues :  - Background color is not correctly validated with a non true  color image in function 'imagerotate()'. (CVE-2008-5498)  - A denial of service condition can be triggered by trying to   extract zip files that contain files with relative paths   in file or directory names.  - Function 'explode()' is affected by an unspecified   vulnerability.  - It may be possible to trigger a segfault by passing a   specially crafted string to function 'json\_decode()'.  - Function 'xml\_error\_string()' is affected by a flaw  which results in messages being off by one. | **Medium** | * Upgrade to PHP version 5.2.9 or later. |
|  | 192.168.1.248 192.168.13.17 | PHP 5.2.10 Multiple Vulnerabilities  - According to its banner, the version of PHP installed on the remote host is older than 5.2.10. Such versions are reportedly affected by multiple vulnerabilities :  - Sufficient checks are not performed on fields reserved   for offsets in function 'exif\_read\_data()'. Successful   exploitation of this issue could result in a denial of   service condition. (bug 48378)  - Provided 'safe\_mode\_exec\_dir' is not set (not set by  default), it may be possible to bypass 'safe\_mode'   restrictions by preceding a backslash in functions   such as 'exec()', 'system()', 'shell\_exec()',   'passthru()' and 'popen()' on a system running PHP   on Windows. (bug 45997) | **Medium** | * Upgrade to PHP version 5.2.10 or later. |
|  | 192.168.1.248 192.168.13.17 | PHP 5.2.12 Multiple Vulnerabilities  - According to its banner, the version of PHP installed on the remote host is older than 5.2.12. Such versions may be affected by several security issues :  - It is possible to bypass the 'safe\_mode' configuration  setting using 'tempnam()'. (CVE-2009-3557)  - It is possible to bypass the 'open\_basedir'   configuration setting using 'posix\_mkfifo()'.   (CVE-2009-3558)  - Provided file uploading is enabled (it is by default),  an attacker can upload files using a POST request with  'multipart/form-data' content even if the target script  doesn't actually support file uploads per se. By   supplying a large number (15,000+) of files, an attacker  could cause the web server to stop responding while it  processes the file list. (CVE-2009-4017)  - Missing protection for '$\_SESSION' from interrupt  corruption and improved 'session.save\_path' check.  (CVE-2009-4143)  - Insufficient input string validation in the   'htmlspecialchars()' function. (CVE-2009-4142) | **Medium** | * Upgrade to PHP version 5.2.12 or later. |
|  | 192.168.1.248 192.168.13.17 | PHP 5.3.2 / 5.2.13 Multiple Vulnerabilities  - According to its banner, the version of PHP installed on the remote host is older than 5.3.2 / 5.2.13. Such versions may be affected by several security issues :  - Directory paths not ending with '/' may not be  correctly validated inside 'tempnam()' in   'safe\_mode' configuration.  - It may be possible to bypass the 'open\_basedir'/   'safe\_mode' configuration restrictions due to an  error in session extensions.  - An unspecified vulnerability affects the LCG entropy. | **Medium** | * Upgrade to PHP version 5.3.2 / 5.2.13 or later. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.16 Multiple Vulnerabilities  - According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.16. It is, therefore, potentially affected by multiple vulnerabilities :  - A denial of service vulnerability in mod\_cache and   mod\_dav. (CVE-2010-1452)    - An information disclosure vulnerability in mod\_proxy\_ajp,  mod\_reqtimeout, and mod\_proxy\_http relating to timeout   conditions. Note that this issue only affects Apache on   Windows, Netware, and OS/2. (CVE-2010-2068) Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves. | **Medium** | * Upgrade to Apache version 2.2.16 or later. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.17 Multiple Vulnerabilities  - According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.17. It is, therefore, affected by the following vulnerabilities :  - Errors exist in the bundled expat library that may allow  an attacker to crash the server when a buffer is over-  read when parsing an XML document. (CVE-2009-3720 and  CVE-2009-3560)  - An error exists in the 'apr\_brigade\_split\_line'   function in the bundled APR-util library. Carefully  timed bytes in requests result in gradual memory  increases leading to a denial of service.   (CVE-2010-1623)   Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves. | **Medium** | * Upgrade to Apache version 2.2.17 or later. Alternatively, ensure that the affected modules are not in use. |
|  | 192.168.1.248 192.168.13.17 | PHP 5.2 5.2.15 Multiple Vulnerabilities  - According to its banner, the version of PHP 5.2 installed on the remote host is older than 5.2.15. Such versions may be affected by several security issues :    - A crash in the zip extract method.  - A possible double free exists in the imap extension.  (CVE-2010-4150)  - An unspecified flaw exists in 'open\_basedir'.   (CVE-2010-3436)  - A possible crash could occur in 'mssql\_fetch\_batch()'.    - A NULL pointer dereference exists in   'ZipArchive::getArchiveComment'. (CVE-2010-3709)  - A crash exists if anti-aliasing steps are invalid.  (Bug #53492)  - A crash exists in pdo\_firebird getAttribute(). (Bug   #53323)  - A user-after-free vulnerability in the Zend engine when  a '\_\_set()', '\_\_get()', '\_\_isset()' or '\_\_unset()'   method is called can allow for a denial of service   attack. (Bug #52879 / CVE-2010-4697)  - A stack-based buffer overflow exists in the   'imagepstext()' function in the GD extension. (Bug   #53492 / CVE-2010-4698)    - The extract function does not prevent use of the  EXTR\_OVERWRITE parameter to overwrite the GLOBALS  superglobal array and the 'this' variable, which  allows attackers to bypass intended access restrictions.  (CVE-2011-0752) | **Medium** | * Upgrade to PHP version 5.2.15 or later. |
|  | 192.168.1.248 192.168.13.17 | PHP 5.2 5.2.17 / 5.3 5.3.5 String To Double Conversion DoS  - According to its banner, the version of PHP 5.x installed on the remote host is older than 5.2.17 or 5.3.5.  Such versions may experience a crash while performing string to double conversion for certain numeric values. Only x86 32-bit PHP processes are known to be affected by this issue regardless of whether the system running PHP is 32-bit or 64-bit. | **Medium** | * Upgrade to PHP 5.2.17/5.3.5 or later. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.18 APR apr\_fnmatch DoS  - According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.18. It is, therefore, affected by a denial of service vulnerability due to an error in the apr\_fnmatch() function of the bundled APR library.  If mod\_autoindex is enabled and has indexed a directory containing files whose filenames are long, an attacker can cause high CPU usage with a specially crafted request.  Note that the remote web server may not actually be affected by this vulnerability. Nessus did not try to determine whether the affected module is in use or to check for the issue itself. | **Medium** | * Upgrade to Apache version 2.2.18 or later. Alternatively, ensure that the 'IndexOptions' configuration option is set to 'IgnoreClient'. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.21 mod\_proxy\_ajp DoS  - According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.21. It is, therefore, potentially affected by a denial of service vulnerability. An error exists in the 'mod\_proxy\_ajp' module that can allow specially crafted HTTP requests to cause a backend server to temporarily enter an error state. This vulnerability only occurs when 'mod\_proxy\_ajp' is used along with 'mod\_proxy\_balancer'. Note that Nessus did not actually test for the flaws but instead has relied on the version in the server's banner. | **Medium** | * Upgrade to Apache version 2.2.21 or later. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.22 Multiple Vulnerabilities  - According to its banner, the version of Apache 2.2.x installed on the remote host is prior to 2.2.22. It is, therefore, potentially affected by the following vulnerabilities :  - When configured as a reverse proxy, improper use of the  RewriteRule and ProxyPassMatch directives could cause  the web server to proxy requests to arbitrary hosts.  This could allow a remote attacker to indirectly send  requests to intranet servers.  (CVE-2011-3368, CVE-2011-4317)  - A heap-based buffer overflow exists when mod\_setenvif  module is enabled and both a maliciously crafted   'SetEnvIf' directive and a maliciously crafted HTTP   request header are used. (CVE-2011-3607)  - A format string handling error can allow the server to  be crashed via maliciously crafted cookies.  (CVE-2012-0021)  - An error exists in 'scoreboard.c' that can allow local  attackers to crash the server during shutdown.  (CVE-2012-0031)  - An error exists in 'protocol.c' that can allow   'HTTPOnly' cookies to be exposed to attackers through  the malicious use of either long or malformed HTTP  headers. (CVE-2012-0053)  - An error in the mod\_proxy\_ajp module when used to   connect to a backend server that takes an overly long   time to respond could lead to a temporary denial of   service. (CVE-2012-4557) Note that Nessus did not actually test for these flaws, but instead  has relied on the version in the server's banner. | **Medium** | * Upgrade to Apache version 2.2.22 or later. |
|  | 192.168.1.248 192.168.13.17 | PHP 5.3.11 Multiple Vulnerabilities  - According to its banner, the version of PHP installed on the remote host is earlier than 5.3.11, and as such is potentially affected by multiple vulnerabilities :  - During the import of environment variables, temporary  changes to the 'magic\_quotes\_gpc' directive are not  handled properly. This can lower the difficulty for  SQL injection attacks. (CVE-2012-0831)  - The '$\_FILES' variable can be corrupted because the  names of uploaded files are not properly validated.  (CVE-2012-1172)  - The 'open\_basedir' directive is not properly handled by  the functions 'readline\_write\_history' and  'readline\_read\_history'.  - The 'header()' function does not detect multi-line  headers with a CR. (Bug #60227 / CVE-2011-1398) | **Medium** | * Upgrade to PHP version 5.3.11 or later. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.23 Multiple Vulnerabilities  - According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.23. It is, therefore, potentially affected by the following vulnerabilities :  - 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)  - An input validation error exists related to  'mod\_negotiation', 'Multiviews' and untrusted uploads  that can allow cross-site scripting attacks.  (CVE-2012-2687) Note that Nessus has not tested for these flaws but has instead relied on the version in the server's banner. | **Medium** | * Upgrade to Apache version 2.2.23 or later. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.24 Multiple XSS Vulnerabilities  - According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.24. It is, therefore, potentially affected by the following cross-site scripting vulnerabilities :  - Errors exist related to the modules mod\_info,  mod\_status, mod\_imagemap, mod\_ldap, and mod\_proxy\_ftp  and unescaped hostnames and URIs that could allow cross-  site scripting attacks. (CVE-2012-3499)  - An error exists related to the mod\_proxy\_balancer  module's manager interface that could allow cross-site  scripting attacks. (CVE-2012-4558) Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner. | **Medium** | * Upgrade to Apache version 2.2.24 or later. Alternatively, ensure that the affected modules are not in use. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.25 Multiple Vulnerabilities  - According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.25. It is, therefore, potentially affected by the following vulnerabilities :  - A flaw exists in the 'RewriteLog' function where it  fails to sanitize escape sequences from being written  to log files, making it potentially vulnerable to  arbitrary command execution. (CVE-2013-1862)  - A denial of service vulnerability exists relating to  the 'mod\_dav' module as it relates to MERGE requests.  (CVE-2013-1896) Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner. | **Medium** | * Upgrade to Apache version 2.2.25 or later. Alternatively, ensure that the affected modules are not in use. |
|  | 192.168.1.248 192.168.13.17 | PHP PHP\_RSHUTDOWN\_FUNCTION Security Bypass  - According to its banner, the version of PHP 5.x installed on the remote host is 5.x prior to 5.3.11 or 5.4.x prior to 5.4.1 and thus, is potentially affected by a security bypass vulnerability. An error exists related to the function 'PHP\_RSHUTDOWN\_FUNCTION' in the libxml extension and the 'stream\_close' method that could allow a remote attacker to bypass 'open\_basedir' protections and obtain sensitive information. Note that this plugin has not attempted to exploit this issue, but has instead relied only on PHP's self-reported version number. | **Medium** | * Upgrade to PHP version 5.3.11 / 5.4.1 or later. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.27 Multiple Vulnerabilities  - According to its banner, the version of Apache 2.2.x running on the remote host is a version prior to 2.2.27. It is, therefore, potentially affected by the following vulnerabilities :  - A flaw exists with the 'mod\_dav' module that is caused  when tracking the length of CDATA that has leading white  space. A remote attacker with a specially crafted DAV  WRITE request can cause the service to stop responding.  (CVE-2013-6438)  - A flaw exists in 'mod\_log\_config' module that is caused  when logging a cookie that has an unassigned value. A  remote attacker with a specially crafted request can  cause the service to crash. (CVE-2014-0098) Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner. | **Medium** | * Upgrade to Apache version 2.2.27 or later. Alternatively, ensure that the affected modules are not in use. |
|  | 192.168.1.248 192.168.13.17 | Apache 2.2.x 2.2.28 Multiple Vulnerabilities  - According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.28. It is, therefore, affected by the following vulnerabilities :  - A flaw exists within the 'mod\_headers' module which  allows a remote attacker to inject arbitrary headers.  This is done by placing a header in the trailer portion  of data being sent using chunked transfer encoding.  (CVE-2013-5704)  - A flaw exists within the 'mod\_deflate' module when  handling highly compressed bodies. Using a specially  crafted request, a remote attacker can exploit this to  cause a denial of service by exhausting memory and CPU  resources. (CVE-2014-0118)  - The 'mod\_status' module contains a race condition that  can be triggered when handling the scoreboard. A remote  attacker can exploit this to cause a denial of service,  execute arbitrary code, or obtain sensitive credential  information. (CVE-2014-0226)  - The 'mod\_cgid' module lacks a time out mechanism. Using  a specially crafted request, a remote attacker can use  this flaw to cause a denial of service by causing child  processes to linger indefinitely, eventually filling up  the scoreboard. (CVE-2014-0231) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | **Medium** | * Upgrade to Apache version 2.2.29 or later. Note that version 2.2.28 was never officially released. |
|  | 192.168.1.248 192.168.13.17 | PHP 7.3.24 Multiple Vulnerabilities  - According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.24. It is, therefore affected by multiple vulnerabilities | **Medium** | * Upgrade to PHP version 7.3.24 or later. |
|  | 192.168.1.248 192.168.13.17 | PHP 7.3.28 Email Header Injection  - According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.28. It is, therefore affected by an email header injection vulnerability, due to a failure to properly handle CR-LF sequences in header fields. An unauthenticated, remote attacker can exploit this, by inserting line feed characters into email headers, to gain full control of email header content. | **Medium** | * Upgrade to PHP version 7.3.28 or later. |
|  | 192.168.1.62 192.168.1.63 192.168.1.68 192.168.1.254 192.168.3.220 192.168.3.231 192.168.3.232 192.168.13.20 | SSL Certificate Expiry  - This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired. | **Medium** | * Purchase or generate a new SSL certificate to replace the existing one. |
|  | 192.168.1.32 192.168.1.33 192.168.1.34 192.168.1.35 192.168.1.36 192.168.1.37 192.168.1.38 192.168.1.39 192.168.1.40 192.168.1.41 192.168.1.42 192.168.1.43 192.168.1.44 192.168.1.45 192.168.1.81 192.168.2.61 192.168.2.62 192.168.2.63 192.168.2.64 192.168.2.65 192.168.2.66 192.168.2.67 192.168.2.68 192.168.2.69 192.168.2.70 192.168.2.71 192.168.2.72 192.168.2.73 192.168.3.118 192.168.3.119 192.168.3.120 192.168.3.121 192.168.3.122 192.168.3.123 192.168.3.124 192.168.3.127 192.168.3.129 192.168.3.131 192.168.3.132 192.168.3.133 192.168.3.134 | Modbus/TCP Coil Access  - 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. | **Medium** | * Restrict access to the Modbus port (TCP/502) to authorized Modbus clients. |
|  | 192.168.1.32 192.168.1.33 192.168.1.34 192.168.1.35 192.168.1.36 192.168.1.37 192.168.1.38 192.168.1.39 192.168.1.40 192.168.1.41 192.168.1.45 192.168.1.81 192.168.2.61 192.168.2.63 192.168.2.64 192.168.2.65 192.168.2.66 192.168.2.67 192.168.2.68 192.168.2.69 192.168.2.70 192.168.2.71 192.168.2.72 192.168.2.73 192.168.3.117 192.168.3.120 192.168.3.121 192.168.3.122 192.168.3.127 192.168.3.128 192.168.3.129 192.168.3.130 192.168.3.131 192.168.3.132 192.168.3.134 | Modbus/TCP Device Identification  - 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. | **Medium** | * Restrict access to the Modbus port (TCP/502) to authorized Modbus clients. |
|  | 192.168.1.34 192.168.1.38 192.168.1.42 192.168.1.43 192.168.1.44 192.168.3.117 192.168.3.118 192.168.3.119 192.168.3.120 192.168.3.121 192.168.3.122 192.168.3.123 192.168.3.124 | Modbus/TCP Discrete Input Access  - 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. | **Medium** | * Restrict access to the Modbus port (TCP/502) to authorized Modbus clients. |
|  | 192.168.1.48 192.168.1.60 192.168.1.62 192.168.1.63 192.168.1.68 192.168.3.80 | Unencrypted Telnet Server  - 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. | **Medium** | * Disable the Telnet service and use SSH instead. |
|  | 192.168.1.62 192.168.1.63 192.168.1.68 | SSL Weak Cipher Suites Supported  - The remote host supports the use of SSL ciphers that offer weak encryption.  Note: This is considerably easier to exploit if the attacker is on the same physical network. | **Medium** | * Reconfigure the affected application, if possible to avoid the use of weak ciphers. |
|  | 192.168.1.62 192.168.1.63 192.168.1.68 192.168.13.11 192.168.13.20 192.168.13.22 192.168.13.23 | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)  - 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. | **Medium** | * Disable SSLv3.  Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled. |
|  | 192.168.2.86 192.168.2.131 192.168.2.147 192.168.2.178 192.168.2.195 192.168.2.211 192.168.2.221 192.168.2.228 | OpenSSL 1.1.1 1.1.1c Vulnerability  - The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the 1.1.1c advisory.  - ChaCha20-Poly1305 is an AEAD cipher, and requires a  unique nonce input for every encryption operation. RFC  7539 specifies that the nonce value (IV) should be 96  bits (12 bytes). OpenSSL allows a variable nonce length  and front pads the nonce with 0 bytes if it is less than  12 bytes. However it also incorrectly allows a nonce to  be set of up to 16 bytes. In this case only the last 12  bytes are significant and any additional leading bytes  are ignored. It is a requirement of using this cipher  that nonce values are unique. Messages encrypted using a  reused nonce value are susceptible to serious  confidentiality and integrity attacks. If an application  changes the default nonce length to be longer than 12  bytes and then makes a change to the leading bytes of  the nonce expecting the new value to be a new unique  nonce then such an application could inadvertently  encrypt messages with a reused nonce. Additionally the  ignored bytes in a long nonce are not covered by the  integrity guarantee of this cipher. Any application that  relies on the integrity of these ignored leading bytes  of a long nonce may be further affected. Any OpenSSL  internal use of this cipher, including in SSL/TLS, is  safe because no such use sets such a long nonce value.  However user applications that use this cipher directly  and set a non-default nonce length to be longer than 12  bytes may be vulnerable. OpenSSL versions 1.1.1 and  1.1.0 are affected by this issue. Due to the limited  scope of affected deployments this has been assessed as  low severity and therefore we are not creating new  releases at this time. (CVE-2019-1543) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | **Medium** | * Upgrade to OpenSSL version 1.1.1c or later. |
|  | 192.168.2.86 192.168.2.131 192.168.2.147 192.168.2.178 192.168.2.195 192.168.2.211 192.168.2.221 192.168.2.228 | OpenSSL 1.1.1 1.1.1d Multiple Vulnerabilities  - The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by the following vulnerabilities :   - Normally in OpenSSL EC groups always have a co-factor  present and this is used in side channel resistant code  paths. However, in some cases, it is possible to  construct a group using explicit parameters (instead of  using a named curve). In those cases it is possible  that such a group does not have the cofactor present.  This can occur even where all the parameters match a  known named curve. If such a curve is used then  OpenSSL falls back to non-side channel resistant code  paths which may result in full key recovery during an  ECDSA signature operation. In order to be vulnerable an  attacker would have to have the ability to time the  creation of a large number of signatures where explicit  parameters with no co-factor present are in use by an  application using libcrypto. For the avoidance of doubt  libssl is not vulnerable because explicit parameters are  never used. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are  affected by this issue. (CVE-2019-1547)   - OpenSSL 1.1.1 introduced a rewritten random number  generator (RNG). This was intended to include protection  in the event of a fork() system call in order to ensure  that the parent and child processes did not share the  same RNG state. However this protection was not being  used in the default case. A partial mitigation for this  issue is that the output from a high precision timer is  mixed into the RNG state so the likelihood of a parent  and child process sharing state is significantly  reduced. If an application already calls  OPENSSL\_init\_crypto() explicitly using  OPENSSL\_INIT\_ATFORK then this problem does not occur at  all. OpenSSL version 1.1.1 is affected by this issue.  (CVE-2019-1549)   - In situations where an attacker receives automated  notification of the success or failure of a decryption  attempt an attacker, after sending a very large number  of messages to be decrypted, can recover a CMS/PKCS7  transported encryption key or decrypt any RSA encrypted  message that was encrypted with the public RSA key,  using a Bleichenbacher padding oracle attack.  Applications are not affected if they use a certificate  together with the private RSA key to the CMS\_decrypt or  PKCS7\_decrypt functions to select the correct recipient  info to decrypt. (CVE-2019-1563)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | **Medium** | * Upgrade to OpenSSL version 1.1.1d or later. |
|  | 192.168.2.86 192.168.2.131 192.168.2.147 192.168.2.178 192.168.2.195 192.168.2.211 192.168.2.221 192.168.2.228 | OpenSSL 1.1.1 1.1.1e-dev Procedure Overflow Vulnerability  - The version of OpenSSL installed on the remote host is prior to 1.1.1e-dev. It is, therefore, affected by a vulnerability as referenced in the 1.1.1e-dev advisory.   - There is an overflow bug in the x64\_64 Montgomery  squaring procedure used in exponentiation with 512-bit  moduli. No EC algorithms are affected. Analysis suggests  that attacks against 2-prime RSA1024, 3-prime RSA1536,  and DSA1024 as a result of this defect would be very  difficult to perform and are not believed likely.  Attacks against DH512 are considered just feasible.  However, for an attack the target would have to re-use  the DH512 private key, which is not recommended anyway.  Also applications directly using the low level API  BN\_mod\_exp may be affected if they use BN\_FLG\_CONSTTIME.  Fixed in OpenSSL 1.1.1e-dev (Affected 1.1.1-1.1.1d).  (CVE-2019-1551)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | **Medium** | * Upgrade to OpenSSL version 1.1.1e-dev or later. |
|  | 192.168.2.86 192.168.2.131 192.168.2.147 192.168.2.178 192.168.2.195 192.168.2.211 192.168.2.221 192.168.2.228 | OpenSSL 1.1.1 1.1.1i Null Pointer Dereference Vulnerability  - The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the 1.1.1i advisory.   - The X.509 GeneralName type is a generic type for representing different types of names. One of those name  types is known as EDIPartyName. OpenSSL provides a function GENERAL\_NAME\_cmp which compares different  instances of a GENERAL\_NAME to see if they are equal or not. This function behaves incorrectly when both  GENERAL\_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a  possible denial of service attack. OpenSSL itself uses the GENERAL\_NAME\_cmp function for two purposes: 1)  Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in  an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp  authority name (exposed via the API functions TS\_RESP\_verify\_response and TS\_RESP\_verify\_token) If an  attacker can control both items being compared then that attacker could trigger a crash. For example if  the attacker can trick a client or server into checking a malicious certificate against a malicious CRL  then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a  certificate. This checking happens prior to the signatures on the certificate and CRL being verified.  OpenSSL's s\_server, s\_client and verify tools have support for the -crl\_download option which implements  automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an  unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of  EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will  accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue.  Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected  1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w). (CVE-2020-1971)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | **Medium** | * Upgrade to OpenSSL version 1.1.1i or later. |
|  | 192.168.2.86 192.168.2.131 192.168.2.147 192.168.2.178 192.168.2.195 192.168.2.211 192.168.2.221 192.168.2.228 | OpenSSL 1.1.1 1.1.1k Multiple Vulnerabilities  - The version of OpenSSL installed on the remote host is prior to 1.1.1k. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.1.1k advisory.   - The X509\_V\_FLAG\_X509\_STRICT flag enables additional security checks of the certificates present in a  certificate chain. It is not set by default. Starting from OpenSSL version 1.1.1h a check to disallow  certificates in the chain that have explicitly encoded elliptic curve parameters was added as an  additional strict check. An error in the implementation of this check meant that the result of a previous  check to confirm that certificates in the chain are valid CA certificates was overwritten. This  effectively bypasses the check that non-CA certificates must not be able to issue other certificates. If a  purpose has been configured then there is a subsequent opportunity for checks that the certificate is a  valid CA. All of the named purpose values implemented in libcrypto perform this check. Therefore, where  a purpose is set the certificate chain will still be rejected even when the strict flag has been used. A  purpose is set by default in libssl client and server certificate verification routines, but it can be  overridden or removed by an application. In order to be affected, an application must explicitly set the  X509\_V\_FLAG\_X509\_STRICT verification flag and either not set a purpose for the certificate verification  or, in the case of TLS client or server applications, override the default purpose. OpenSSL versions  1.1.1h and newer are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k.  OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1h-1.1.1j).  (CVE-2021-3450)   - An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a  client. If a TLSv1.2 renegotiation ClientHello omits the signature\_algorithms extension (where it was  present in the initial ClientHello), but includes a signature\_algorithms\_cert extension then a NULL  pointer dereference will result, leading to a crash and a denial of service attack. A server is only  vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration). OpenSSL TLS  clients are not impacted by this issue. All OpenSSL 1.1.1 versions are affected by this issue. Users of  these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in  OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j). (CVE-2021-3449)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | **Medium** | * Upgrade to OpenSSL version 1.1.1k or later. |
|  | 192.168.2.86 192.168.2.131 192.168.2.147 192.168.2.178 192.168.2.195 192.168.2.211 192.168.2.221 192.168.2.228 | OpenSSL 1.1.1 1.1.1j Multiple Vulnerabilities  - The version of OpenSSL installed on the remote host is prior to 1.1.1j. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.1.1j advisory.   - The OpenSSL public API function X509\_issuer\_and\_serial\_hash() attempts to create a unique hash value based  on the issuer and serial number data contained within an X509 certificate. However it fails to correctly  handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is  maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a  potential denial of service attack. The function X509\_issuer\_and\_serial\_hash() is never directly called by  OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on  certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are  affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x  and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving  public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should  upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected  1.0.2-1.0.2x). (CVE-2021-23841)   - Calls to EVP\_CipherUpdate, EVP\_EncryptUpdate and EVP\_DecryptUpdate may overflow the output length argument  in some cases where the input length is close to the maximum permissable length for an integer on the  platform. In such cases the return value from the function call will be 1 (indicating success), but the  output length value will be negative. This could cause applications to behave incorrectly or crash.  OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to  OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out  of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should  upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i).  Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x). (CVE-2021-23840)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | **Medium** | * Upgrade to OpenSSL version 1.1.1j or later. |
|  | 192.168.2.86 192.168.2.131 192.168.2.147 192.168.2.178 192.168.2.195 192.168.2.211 192.168.2.221 192.168.2.228 | OpenSSL 1.1.1 1.1.1m Vulnerability  - The version of OpenSSL installed on the remote host is prior to 1.1.1m. It is, therefore, affected by a vulnerability as referenced in the 1.1.1m advisory.   - There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are  affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the  pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that  attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not  believed likely. Attacks against DH are considered just feasible (although very difficult) because most of  the work necessary to deduce information about a private key may be performed offline. The amount of  resources required for such an attack would be significant. However, for an attack on TLS to be  meaningful, the server would have to share the DH private key among multiple clients, which is no longer  an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was  addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is  addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made  available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in  OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). (CVE-2021-4160)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | **Medium** | * Upgrade to OpenSSL version 1.1.1m or later. |
|  | 192.168.2.217 | OpenSSL 1.0.x 1.0.2r Information Disclosure Vulnerability  - According to its banner, the version of OpenSSL running on the remote host is 1.0.x prior to 1.0.2r. It is, therefore, affected by an information disclosure vulnerability due to the decipherable way a application responds to a 0 byte record. An unauthenticated, remote attacker could exploit this vulnerability, via a padding oracle attack, to potentially disclose sensitive information. Note: Only 'non-stitched' ciphersuites are exploitable. | **Medium** | * Upgrade to OpenSSL version 1.0.2r or later. |
|  | 192.168.2.217 | OpenSSL 1.0.2 1.0.2t Multiple Vulnerabilities  - The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by multiple vulnerabilities :  - Normally in OpenSSL EC groups always have a co-factor  present and this is used in side channel resistant code  paths. However, in some cases, it is possible to  construct a group using explicit parameters (instead of  using a named curve). In those cases it is possible  that such a group does not have the cofactor present.  This can occur even where all the parameters match a  known named curve. If such a curve is used then  OpenSSL falls back to non-side channel resistant code  paths which may result in full key recovery during an  ECDSA signature operation. In order to be vulnerable an  attacker would have to have the ability to time the  creation of a large number of signatures where explicit  parameters with no co-factor present are in use by an  application using libcrypto. For the avoidance of doubt  libssl is not vulnerable because explicit parameters are  never used. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are  affected by this issue. (CVE-2019-1547)  - OpenSSL has internal defaults for a directory tree where  it can find a configuration file as well as certificates  used for verification in TLS. This directory is most  commonly referred to as OPENSSLDIR, and is configurable  with the --prefix / --openssldir configuration options.  For OpenSSL versions 1.1.0 and 1.1.1, the mingw  configuration targets assume that resulting programs and  libraries are installed in a Unix-like environment and  the default prefix for program installation as well as  for OPENSSLDIR should be '/usr/local'. However, mingw  programs are Windows programs, and as such, find  themselves looking at sub-directories of 'C:/usr/local',  which may be world writable, which enables untrusted  users to modify OpenSSL's default configuration, insert  CA certificates, modify (or even replace) existing  engine modules, etc. For OpenSSL 1.0.2, '/usr/local/ssl'  is used as default for OPENSSLDIR on all Unix and  Windows targets, including Visual C builds. However,  some build instructions for the diverse Windows targets  on 1.0.2 encourage you to specify your own --prefix.  OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by  this issue. Due to the limited scope of affected  deployments this has been assessed as low severity and  therefore we are not creating new releases at this time.  (CVE-2019-1552)  - In situations where an attacker receives automated  notification of the success or failure of a decryption  attempt an attacker, after sending a very large number  of messages to be decrypted, can recover a CMS/PKCS7  transported encryption key or decrypt any RSA encrypted  message that was encrypted with the public RSA key,  using a Bleichenbacher padding oracle attack.  Applications are not affected if they use a certificate  together with the private RSA key to the CMS\_decrypt or  PKCS7\_decrypt functions to select the correct recipient  info to decrypt. (CVE-2019-1563) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | **Medium** | * Upgrade to OpenSSL version 1.0.2t or later. |
|  | 192.168.2.217 | OpenSSL 1.0.2 1.0.2u Procedure Overflow Vulnerability  - The version of OpenSSL installed on the remote host is prior to 1.0.2u. It is, therefore, affected by a vulnerability as referenced in the 1.0.2u advisory.  - There is an overflow bug in the x64\_64 Montgomery  squaring procedure used in exponentiation with 512-bit  moduli. No EC algorithms are affected. Analysis suggests  that attacks against 2-prime RSA1024, 3-prime RSA1536,  and DSA1024 as a result of this defect would be very  difficult to perform and are not believed likely.  Attacks against DH512 are considered just feasible.  However, for an attack the target would have to re-use  the DH512 private key, which is not recommended anyway.  Also applications directly using the low level API  BN\_mod\_exp may be affected if they use BN\_FLG\_CONSTTIME.  Fixed in OpenSSL 1.1.1e-dev (Affected 1.1.1-1.1.1d).  Fixed in OpenSSL 1.0.2u-dev (Affected 1.0.2-1.0.2t).  (CVE-2019-1551) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | **Medium** | * Upgrade to OpenSSL version 1.0.2u or later. |
|  | 192.168.2.217 | OpenSSL 1.0.2 1.0.2x Null Pointer Dereference Vulnerability  - The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the 1.0.2x advisory.  - The X.509 GeneralName type is a generic type for representing different types of names. One of those name  types is known as EDIPartyName. OpenSSL provides a function GENERAL\_NAME\_cmp which compares different  instances of a GENERAL\_NAME to see if they are equal or not. This function behaves incorrectly when both  GENERAL\_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a  possible denial of service attack. OpenSSL itself uses the GENERAL\_NAME\_cmp function for two purposes: 1)  Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in  an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp  authority name (exposed via the API functions TS\_RESP\_verify\_response and TS\_RESP\_verify\_token) If an  attacker can control both items being compared then that attacker could trigger a crash. For example if  the attacker can trick a client or server into checking a malicious certificate against a malicious CRL  then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a  certificate. This checking happens prior to the signatures on the certificate and CRL being verified.  OpenSSL's s\_server, s\_client and verify tools have support for the -crl\_download option which implements  automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an  unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of  EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will  accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue.  Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected  1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w). (CVE-2020-1971) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | **Medium** | * Upgrade to OpenSSL version 1.0.2x or later. |
|  | 192.168.2.217 | OpenSSL 1.0.2 1.0.2w Information Disclosure  - The version of OpenSSL installed on the remote host is 1.0.2 prior to 1.0.2w. It is, therefore, affected by a vulnerability as referenced in the 1.0.2w advisory. The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over that TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connections. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | **Medium** | * Upgrade to OpenSSL version 1.0.2w or later. |
|  | 192.168.2.217 | OpenSSL 1.0.2 1.0.2y Multiple Vulnerabilities  - The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.0.2y advisory.  - The OpenSSL public API function X509\_issuer\_and\_serial\_hash() attempts to create a unique hash value based  on the issuer and serial number data contained within an X509 certificate. However it fails to correctly  handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is  maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a  potential denial of service attack. The function X509\_issuer\_and\_serial\_hash() is never directly called by  OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on  certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are  affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x  and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving  public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should  upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected  1.0.2-1.0.2x). (CVE-2021-23841)  - Calls to EVP\_CipherUpdate, EVP\_EncryptUpdate and EVP\_DecryptUpdate may overflow the output length argument  in some cases where the input length is close to the maximum permissable length for an integer on the  platform. In such cases the return value from the function call will be 1 (indicating success), but the  output length value will be negative. This could cause applications to behave incorrectly or crash.  OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to  OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out  of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should  upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i).  Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x). (CVE-2021-23840)  - OpenSSL 1.0.2 supports SSLv2. If a client attempts to negotiate SSLv2 with a server that is configured to  support both SSLv2 and more recent SSL and TLS versions then a check is made for a version rollback attack  when unpadding an RSA signature. Clients that support SSL or TLS versions greater than SSLv2 are supposed  to use a special form of padding. A server that supports greater than SSLv2 is supposed to reject  connection attempts from a client where this special form of padding is present, because this indicates  that a version rollback has occurred (i.e. both client and server support greater than SSLv2, and yet this  is the version that is being requested). The implementation of this padding check inverted the logic so  that the connection attempt is accepted if the padding is present, and rejected if it is absent. This  means that such as server will accept a connection if a version rollback attack has occurred. Further the  server will erroneously reject a connection if a normal SSLv2 connection attempt is made. Only OpenSSL  1.0.2 servers from version 1.0.2s to 1.0.2x are affected by this issue. In order to be vulnerable a 1.0.2  server must: 1) have configured SSLv2 support at compile time (this is off by default), 2) have configured  SSLv2 support at runtime (this is off by default), 3) have configured SSLv2 ciphersuites (these are not in  the default ciphersuite list) OpenSSL 1.1.1 does not have SSLv2 support and therefore is not vulnerable to  this issue. The underlying error is in the implementation of the RSA\_padding\_check\_SSLv23() function. This  also affects the RSA\_SSLV23\_PADDING padding mode used by various other functions. Although 1.1.1 does not  support SSLv2 the RSA\_padding\_check\_SSLv23() function still exists, as does the RSA\_SSLV23\_PADDING padding  mode. Applications that directly call that function or use that padding mode will encounter this issue.  However since there is no support for the SSLv2 protocol in 1.1.1 this is considered a bug and not a  security issue in that version. OpenSSL 1.0.2 is out of support and no longer receiving public updates.  Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j.  Fixed in OpenSSL 1.0.2y (Affected 1.0.2s-1.0.2x). (CVE-2021-23839) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | **Medium** | * Upgrade to OpenSSL version 1.0.2y or later. |
|  | 192.168.2.217 | OpenSSL 1.0.2 1.0.2za Vulnerability  - The version of OpenSSL installed on the remote host is prior to 1.0.2za. It is, therefore, affected by a vulnerability as referenced in the 1.0.2za advisory.  - ASN.1 strings are represented internally within OpenSSL as an ASN1\_STRING structure which contains a  buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings  which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not  a strict requirement, ASN.1 strings that are parsed using OpenSSL's own d2i functions (and other similar  parsing functions) as well as any string whose value has been set with the ASN1\_STRING\_set() function will  additionally NUL terminate the byte array in the ASN1\_STRING structure. However, it is possible for  applications to directly construct valid ASN1\_STRING structures which do not NUL terminate the byte array  by directly setting the data and length fields in the ASN1\_STRING array. This can also happen by using  the ASN1\_STRING\_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to  assume that the ASN1\_STRING byte array will be NUL terminated, even though this is not guaranteed for  strings that have been directly constructed. Where an application requests an ASN.1 structure to be  printed, and where that ASN.1 structure contains ASN1\_STRINGs that have been directly constructed by the  application without NUL terminating the data field, then a read buffer overrun can occur. The same thing  can also occur during name constraints processing of certificates (for example if a certificate has been  directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the  certificate contains non NUL terminated ASN1\_STRING structures). It can also occur in the  X509\_get1\_email(), X509\_REQ\_get1\_email() and X509\_get1\_ocsp() functions. If a malicious actor can cause an  application to directly construct an ASN1\_STRING and then process it through one of the affected OpenSSL  functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack).  It could also result in the disclosure of private memory contents (such as private keys, or sensitive  plaintext). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y). (CVE-2021-3712) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | **Medium** | * Upgrade to OpenSSL version 1.0.2za or later. |
|  | 192.168.2.217 | OpenSSL 1.0.2 1.0.2zc-dev Vulnerability  - The version of OpenSSL installed on the remote host is prior to 1.0.2zc-dev. It is, therefore, affected by a vulnerability as referenced in the 1.0.2zc-dev advisory.  - There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are  affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the  pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that  attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not  believed likely. Attacks against DH are considered just feasible (although very difficult) because most of  the work necessary to deduce information about a private key may be performed offline. The amount of  resources required for such an attack would be significant. However, for an attack on TLS to be  meaningful, the server would have to share the DH private key among multiple clients, which is no longer  an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was  addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is  addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made  available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in  OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-  dev (Affected 1.0.2-1.0.2zb). (CVE-2021-4160) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | **Medium** | * Upgrade to OpenSSL version 1.0.2zc-dev or later. |
|  | 192.168.3.120 192.168.3.121 192.168.3.122 192.168.3.127 192.168.3.129 192.168.3.131 192.168.3.132 192.168.3.134 | Modbus/TCP Report Slave ID  - Nessus sent a Modbus Report Slave ID function code 17 to obtain the device's Slave ID. | **Medium** | * Restrict access to the Modbus port (TCP/502) to authorized Modbus clients. |
|  | 192.168.3.128 192.168.3.130 | TFTP Traversal Arbitrary File Access  - The TFTP (Trivial File Transfer Protocol) server running on the remote host is vulnerable to a directory traversal attack that allows an attacker to read arbitrary files on the remote host by prepending their names with directory traversal sequences. | **Medium** | * Disable the remote TFTP daemon, run it in a chrooted environment, or filter incoming traffic to this port. |
|  | 192.168.3.128 192.168.3.130 | Dropbear SSH Server 2013.59 Multiple Vulnerabilities  - According to its self-reported banner, the version of Dropbear SSH running on this port is earlier than 2013.59. As such, it is potentially affected by multiple vulnerabilities :  - A denial of service vulnerability caused by the way the  'buf\_decompress()' function handles compressed files.  (CVE-2013-4421)  - User-enumeration is possible due to a timing error when  authenticating users. (CVE-2013-4434) | **Medium** | * Upgrade to the Dropbear SSH 2013.59 or later. |
|  | 192.168.3.161 | MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)  - 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. | **Medium** | * Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10. |
|  | 192.168.1.21 192.168.1.101 192.168.3.161 192.168.3.162 | Terminal Services Encryption Level is not FIPS-140 Compliant  - The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant. | **Low** | * Change RDP encryption level to :  4. FIPS Compliant |
|  | 192.168.1.11 192.168.1.62 192.168.1.63 192.168.1.68 192.168.2.86 192.168.2.131 192.168.2.147 192.168.2.195 192.168.2.217 192.168.2.221 192.168.2.228 192.168.13.11 192.168.13.22 192.168.13.23 | SSL Certificate Chain Contains RSA Keys Less Than 2048 bits  - 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. | **Low** | * 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. |
|  | 192.168.1.21 192.168.3.161 | SMTP Service Cleartext Login Permitted  - The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used. | **Low** | * Configure the service to support less secure authentication mechanisms only over an encrypted channel. |
|  | 192.168.1.48 | Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)  - The remote host uses a network device driver that pads ethernet frames with data which vary from one packet to another, likely taken from kernel memory, system memory allocated to the device driver, or a hardware buffer on its network interface card. Known as 'Etherleak', this information disclosure vulnerability may allow an attacker to collect sensitive information from the affected host provided he is on the same physical subnet as that host. | **Low** | * Contact the network device driver's vendor for a fix. |
|  | 192.168.3.128 192.168.3.130 | SSH Server CBC Mode Ciphers Enabled  - 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. | **Low** | * Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption. |
|  | 192.168.3.128 192.168.3.130 | SSH Weak MAC Algorithms Enabled  - 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. | **Low** | * Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms. |
|  | 192.168.3.128 192.168.3.130 | SSH Weak Key Exchange Algorithms Enabled  - 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. | **Low** | * Contact the vendor or consult product documentation to disable the weak algorithms. |
|  | 192.168.13.17 | SSL/TLS Diffie-Hellman Modulus = 1024 Bits (Logjam)  - 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. | **Low** | * Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater. |

**ตารางที่ 3** รายละเอียดช่องโหว่พร้อมแนวทางการแก้ไข

## ภาคผนวก รายละเอียดรายการ IP ที่ดำเนินการตรวจสอบช่องโหว่

| * Phase\_1 |
| --- |

| 192.168.1.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.1.2 | 0 | 0 | 1 | 0 | 1 |
| 2. | 192.168.1.3 | 0 | 0 | 1 | 0 | 1 |
| 3. | 192.168.1.4 | 0 | 0 | 1 | 0 | 1 |
| 4. | 192.168.1.5 | 0 | 0 | 1 | 0 | 1 |
| 5. | 192.168.1.6 | 0 | 0 | 1 | 0 | 1 |
| 6. | 192.168.1.7 | 0 | 0 | 1 | 0 | 1 |
| 7. | 192.168.1.8 | 0 | 0 | 1 | 0 | 1 |
| 8. | 192.168.1.9 | 0 | 0 | 1 | 0 | 1 |
| 9. | 192.168.1.10 | 0 | 0 | 1 | 0 | 1 |
| 10. | 192.168.1.11 | 1 | 0 | 4 | 1 | 6 |
| 11. | 192.168.1.12 | 0 | 0 | 1 | 0 | 1 |
| 12. | 192.168.1.13 | 0 | 0 | 1 | 0 | 1 |
| 13. | 192.168.1.15 | 0 | 0 | 1 | 0 | 1 |
| 14. | 192.168.1.21 | 3 | 0 | 16 | 2 | 21 |
| 15. | 192.168.1.23 | 0 | 1 | 2 | 0 | 3 |
| 16. | 192.168.1.24 | 1 | 1 | 1 | 0 | 3 |
| 17. | 192.168.1.25 | 0 | 1 | 1 | 0 | 2 |
| 18. | 192.168.1.26 | 1 | 1 | 2 | 0 | 4 |
| 19. | 192.168.1.27 | 1 | 1 | 2 | 0 | 4 |
| 20. | 192.168.1.28 | 1 | 1 | 2 | 0 | 4 |
| 21. | 192.168.1.29 | 0 | 1 | 2 | 0 | 3 |
| 22. | 192.168.1.30 | 1 | 1 | 1 | 0 | 3 |
| 23. | 192.168.1.32 | 0 | 0 | 2 | 0 | 2 |
| 24. | 192.168.1.33 | 0 | 0 | 2 | 0 | 2 |
| 25. | 192.168.1.34 | 0 | 0 | 3 | 0 | 3 |
| 26. | 192.168.1.35 | 0 | 0 | 2 | 0 | 2 |
| 27. | 192.168.1.36 | 0 | 0 | 2 | 0 | 2 |
| 28. | 192.168.1.37 | 0 | 0 | 2 | 0 | 2 |
| 29. | 192.168.1.38 | 0 | 0 | 3 | 0 | 3 |
| 30. | 192.168.1.39 | 0 | 0 | 2 | 0 | 2 |
| 31. | 192.168.1.40 | 0 | 0 | 2 | 0 | 2 |
| 32. | 192.168.1.41 | 0 | 0 | 2 | 0 | 2 |
| 33. | 192.168.1.42 | 0 | 0 | 2 | 0 | 2 |
| 34. | 192.168.1.43 | 0 | 0 | 2 | 0 | 2 |
| 35. | 192.168.1.44 | 0 | 0 | 2 | 0 | 2 |
| 36. | 192.168.1.45 | 0 | 0 | 2 | 0 | 2 |
| 37. | 192.168.1.46 | 0 | 1 | 0 | 0 | 1 |
| 38. | 192.168.1.48 | 0 | 1 | 1 | 1 | 3 |
| 39. | 192.168.1.50 | 0 | 0 | 0 | 0 | 0 |
| 40. | 192.168.1.51 | 1 | 1 | 2 | 0 | 4 |
| 41. | 192.168.1.52 | 1 | 1 | 1 | 0 | 3 |
| 42. | 192.168.1.53 | 1 | 1 | 1 | 0 | 3 |
| 43. | 192.168.1.54 | 1 | 1 | 2 | 0 | 4 |
| 44. | 192.168.1.55 | 1 | 1 | 1 | 0 | 3 |
| 45. | 192.168.1.56 | 1 | 1 | 2 | 0 | 4 |
| 46. | 192.168.1.57 | 1 | 1 | 2 | 0 | 4 |
| 47. | 192.168.1.58 | 0 | 1 | 2 | 0 | 3 |
| 48. | 192.168.1.60 | 0 | 2 | 1 | 0 | 3 |
| 49. | 192.168.1.61 | 0 | 0 | 5 | 0 | 5 |
| 50. | 192.168.1.62 | 0 | 1 | 10 | 1 | 12 |
| 51. | 192.168.1.63 | 0 | 1 | 10 | 1 | 12 |
| 52. | 192.168.1.64 | 0 | 0 | 0 | 0 | 0 |
| 53. | 192.168.1.65 | 0 | 0 | 0 | 0 | 0 |
| 54. | 192.168.1.66 | 0 | 0 | 0 | 0 | 0 |
| 55. | 192.168.1.67 | 0 | 0 | 0 | 0 | 0 |
| 56. | 192.168.1.68 | 0 | 1 | 10 | 1 | 12 |
| 57. | 192.168.1.69 | 0 | 0 | 0 | 0 | 0 |
| 58. | 192.168.1.70 | 0 | 0 | 0 | 0 | 0 |
| 59. | 192.168.1.71 | 0 | 0 | 0 | 0 | 0 |
| 60. | 192.168.1.72 | 0 | 0 | 0 | 0 | 0 |
| 61. | 192.168.1.73 | 0 | 0 | 0 | 0 | 0 |
| 62. | 192.168.1.74 | 0 | 0 | 0 | 0 | 0 |
| 63. | 192.168.1.75 | 0 | 0 | 0 | 0 | 0 |
| 64. | 192.168.1.76 | 0 | 0 | 1 | 0 | 1 |
| 65. | 192.168.1.77 | 0 | 0 | 1 | 0 | 1 |
| 66. | 192.168.1.78 | 0 | 0 | 1 | 0 | 1 |
| 67. | 192.168.1.79 | 0 | 0 | 1 | 0 | 1 |
| 68. | 192.168.1.80 | 0 | 0 | 1 | 0 | 1 |
| 69. | 192.168.1.81 | 0 | 0 | 2 | 0 | 2 |
| 70. | 192.168.1.83 | 0 | 0 | 1 | 0 | 1 |
| 71. | 192.168.1.84 | 0 | 0 | 1 | 0 | 1 |
| 72. | 192.168.1.85 | 0 | 0 | 1 | 0 | 1 |
| 73. | 192.168.1.86 | 0 | 0 | 1 | 0 | 1 |
| 74. | 192.168.1.87 | 0 | 0 | 1 | 0 | 1 |
| 75. | 192.168.1.88 | 0 | 0 | 1 | 0 | 1 |
| 76. | 192.168.1.89 | 0 | 1 | 2 | 0 | 3 |
| 77. | 192.168.1.91 | 0 | 0 | 0 | 0 | 0 |
| 78. | 192.168.1.92 | 0 | 0 | 0 | 0 | 0 |
| 79. | 192.168.1.93 | 0 | 0 | 0 | 0 | 0 |
| 80. | 192.168.1.94 | 0 | 0 | 0 | 0 | 0 |
| 81. | 192.168.1.95 | 0 | 0 | 0 | 0 | 0 |
| 82. | 192.168.1.96 | 0 | 0 | 0 | 0 | 0 |
| 83. | 192.168.1.97 | 0 | 0 | 0 | 0 | 0 |
| 84. | 192.168.1.98 | 0 | 0 | 0 | 0 | 0 |
| 85. | 192.168.1.99 | 0 | 0 | 0 | 0 | 0 |
| 86. | 192.168.1.101 | 2 | 0 | 10 | 1 | 13 |
| 87. | 192.168.1.102 | 0 | 0 | 1 | 0 | 1 |
| 88. | 192.168.1.104 | 0 | 0 | 1 | 0 | 1 |
| 89. | 192.168.1.105 | 0 | 0 | 1 | 0 | 1 |
| 90. | 192.168.1.106 | 0 | 0 | 1 | 0 | 1 |
| 91. | 192.168.1.107 | 0 | 0 | 1 | 0 | 1 |
| 92. | 192.168.1.108 | 0 | 0 | 1 | 0 | 1 |
| 93. | 192.168.1.110 | 0 | 0 | 1 | 0 | 1 |
| 94. | 192.168.1.111 | 0 | 0 | 1 | 0 | 1 |
| 95. | 192.168.1.112 | 0 | 0 | 1 | 0 | 1 |
| 96. | 192.168.1.113 | 0 | 0 | 1 | 0 | 1 |
| 97. | 192.168.1.115 | 0 | 0 | 1 | 0 | 1 |
| 98. | 192.168.1.116 | 0 | 0 | 1 | 0 | 1 |
| 99. | 192.168.1.117 | 0 | 0 | 1 | 0 | 1 |
| 100. | 192.168.1.119 | 0 | 0 | 1 | 0 | 1 |
| 101. | 192.168.1.120 | 0 | 0 | 1 | 0 | 1 |
| 102. | 192.168.1.121 | 0 | 0 | 1 | 0 | 1 |
| 103. | 192.168.1.122 | 0 | 0 | 1 | 0 | 1 |
| 104. | 192.168.1.123 | 0 | 0 | 1 | 0 | 1 |
| 105. | 192.168.1.124 | 0 | 0 | 1 | 0 | 1 |
| 106. | 192.168.1.125 | 0 | 0 | 1 | 0 | 1 |
| 107. | 192.168.1.126 | 0 | 0 | 1 | 0 | 1 |
| 108. | 192.168.1.127 | 0 | 0 | 1 | 0 | 1 |
| 109. | 192.168.1.128 | 0 | 0 | 1 | 0 | 1 |
| 110. | 192.168.1.129 | 0 | 0 | 1 | 0 | 1 |
| 111. | 192.168.1.130 | 0 | 0 | 0 | 0 | 0 |
| 112. | 192.168.1.131 | 0 | 0 | 0 | 0 | 0 |
| 113. | 192.168.1.132 | 0 | 0 | 0 | 0 | 0 |
| 114. | 192.168.1.133 | 0 | 0 | 1 | 0 | 1 |
| 115. | 192.168.1.134 | 0 | 0 | 0 | 0 | 0 |
| 116. | 192.168.1.135 | 0 | 0 | 0 | 0 | 0 |
| 117. | 192.168.1.136 | 0 | 0 | 1 | 0 | 1 |
| 118. | 192.168.1.137 | 0 | 0 | 1 | 0 | 1 |
| 119. | 192.168.1.138 | 0 | 0 | 0 | 0 | 0 |
| 120. | 192.168.1.139 | 0 | 0 | 1 | 0 | 1 |
| 121. | 192.168.1.140 | 0 | 0 | 0 | 0 | 0 |
| 122. | 192.168.1.141 | 0 | 0 | 1 | 0 | 1 |
| 123. | 192.168.1.142 | 0 | 0 | 1 | 0 | 1 |
| 124. | 192.168.1.143 | 0 | 0 | 1 | 0 | 1 |
| 125. | 192.168.1.144 | 0 | 0 | 1 | 0 | 1 |
| 126. | 192.168.1.145 | 0 | 0 | 1 | 0 | 1 |
| 127. | 192.168.1.146 | 0 | 0 | 1 | 0 | 1 |
| 128. | 192.168.1.147 | 0 | 0 | 1 | 0 | 1 |
| 129. | 192.168.1.148 | 0 | 0 | 1 | 0 | 1 |
| 130. | 192.168.1.149 | 0 | 0 | 1 | 0 | 1 |
| 131. | 192.168.1.150 | 0 | 0 | 1 | 0 | 1 |
| 132. | 192.168.1.151 | 0 | 0 | 1 | 0 | 1 |
| 133. | 192.168.1.152 | 0 | 0 | 1 | 0 | 1 |
| 134. | 192.168.1.153 | 0 | 0 | 0 | 0 | 0 |
| 135. | 192.168.1.154 | 0 | 0 | 0 | 0 | 0 |
| 136. | 192.168.1.155 | 0 | 0 | 0 | 0 | 0 |
| 137. | 192.168.1.156 | 0 | 0 | 0 | 0 | 0 |
| 138. | 192.168.1.157 | 0 | 0 | 0 | 0 | 0 |
| 139. | 192.168.1.158 | 0 | 0 | 0 | 0 | 0 |
| 140. | 192.168.1.159 | 0 | 0 | 0 | 0 | 0 |
| 141. | 192.168.1.160 | 0 | 0 | 0 | 0 | 0 |
| 142. | 192.168.1.161 | 0 | 0 | 1 | 0 | 1 |
| 143. | 192.168.1.162 | 0 | 0 | 1 | 0 | 1 |
| 144. | 192.168.1.163 | 0 | 0 | 1 | 0 | 1 |
| 145. | 192.168.1.164 | 0 | 0 | 1 | 0 | 1 |
| 146. | 192.168.1.165 | 0 | 0 | 0 | 0 | 0 |
| 147. | 192.168.1.166 | 0 | 0 | 0 | 0 | 0 |
| 148. | 192.168.1.167 | 0 | 0 | 1 | 0 | 1 |
| 149. | 192.168.1.168 | 0 | 0 | 1 | 0 | 1 |
| 150. | 192.168.1.169 | 0 | 0 | 1 | 0 | 1 |
| 151. | 192.168.1.170 | 0 | 0 | 1 | 0 | 1 |
| 152. | 192.168.1.171 | 0 | 0 | 1 | 0 | 1 |
| 153. | 192.168.1.172 | 0 | 0 | 1 | 0 | 1 |
| 154. | 192.168.1.173 | 0 | 0 | 1 | 0 | 1 |
| 155. | 192.168.1.174 | 0 | 0 | 1 | 0 | 1 |
| 156. | 192.168.1.175 | 0 | 0 | 1 | 0 | 1 |
| 157. | 192.168.1.176 | 0 | 0 | 1 | 0 | 1 |
| 158. | 192.168.1.177 | 0 | 0 | 1 | 0 | 1 |
| 159. | 192.168.1.178 | 0 | 0 | 1 | 0 | 1 |
| 160. | 192.168.1.179 | 0 | 0 | 1 | 0 | 1 |
| 161. | 192.168.1.180 | 0 | 0 | 1 | 0 | 1 |
| 162. | 192.168.1.181 | 0 | 0 | 1 | 0 | 1 |
| 163. | 192.168.1.182 | 0 | 0 | 1 | 0 | 1 |
| 164. | 192.168.1.183 | 0 | 0 | 1 | 0 | 1 |
| 165. | 192.168.1.184 | 0 | 0 | 1 | 0 | 1 |
| 166. | 192.168.1.185 | 0 | 0 | 1 | 0 | 1 |
| 167. | 192.168.1.186 | 0 | 0 | 1 | 0 | 1 |
| 168. | 192.168.1.187 | 0 | 0 | 1 | 0 | 1 |
| 169. | 192.168.1.188 | 0 | 0 | 1 | 0 | 1 |
| 170. | 192.168.1.189 | 0 | 0 | 1 | 0 | 1 |
| 171. | 192.168.1.190 | 0 | 0 | 1 | 0 | 1 |
| 172. | 192.168.1.191 | 0 | 0 | 1 | 0 | 1 |
| 173. | 192.168.1.192 | 0 | 0 | 1 | 0 | 1 |
| 174. | 192.168.1.193 | 0 | 0 | 1 | 0 | 1 |
| 175. | 192.168.1.194 | 0 | 0 | 1 | 0 | 1 |
| 176. | 192.168.1.195 | 0 | 0 | 1 | 0 | 1 |
| 177. | 192.168.1.196 | 0 | 0 | 1 | 0 | 1 |
| 178. | 192.168.1.197 | 0 | 0 | 1 | 0 | 1 |
| 179. | 192.168.1.198 | 0 | 0 | 1 | 0 | 1 |
| 180. | 192.168.1.199 | 0 | 0 | 1 | 0 | 1 |
| 181. | 192.168.1.200 | 0 | 0 | 1 | 0 | 1 |
| 182. | 192.168.1.201 | 0 | 0 | 1 | 0 | 1 |
| 183. | 192.168.1.202 | 0 | 0 | 1 | 0 | 1 |
| 184. | 192.168.1.203 | 0 | 0 | 1 | 0 | 1 |
| 185. | 192.168.1.204 | 0 | 0 | 1 | 0 | 1 |
| 186. | 192.168.1.205 | 0 | 0 | 1 | 0 | 1 |
| 187. | 192.168.1.206 | 0 | 0 | 1 | 0 | 1 |
| 188. | 192.168.1.207 | 0 | 0 | 1 | 0 | 1 |
| 189. | 192.168.1.208 | 0 | 0 | 1 | 0 | 1 |
| 190. | 192.168.1.209 | 0 | 0 | 1 | 0 | 1 |
| 191. | 192.168.1.211 | 0 | 0 | 1 | 0 | 1 |
| 192. | 192.168.1.212 | 0 | 0 | 1 | 0 | 1 |
| 193. | 192.168.1.213 | 0 | 0 | 1 | 0 | 1 |
| 194. | 192.168.1.214 | 0 | 0 | 1 | 0 | 1 |
| 195. | 192.168.1.215 | 0 | 0 | 1 | 0 | 1 |
| 196. | 192.168.1.216 | 0 | 0 | 1 | 0 | 1 |
| 197. | 192.168.1.217 | 0 | 0 | 0 | 0 | 0 |
| 198. | 192.168.1.218 | 0 | 0 | 0 | 0 | 0 |
| 199. | 192.168.1.219 | 0 | 0 | 0 | 0 | 0 |
| 200. | 192.168.1.220 | 0 | 0 | 0 | 0 | 0 |
| 201. | 192.168.1.221 | 0 | 0 | 0 | 0 | 0 |
| 202. | 192.168.1.222 | 0 | 0 | 0 | 0 | 0 |
| 203. | 192.168.1.223 | 0 | 0 | 0 | 0 | 0 |
| 204. | 192.168.1.224 | 0 | 0 | 1 | 0 | 1 |
| 205. | 192.168.1.225 | 0 | 0 | 1 | 0 | 1 |
| 206. | 192.168.1.226 | 0 | 0 | 1 | 0 | 1 |
| 207. | 192.168.1.227 | 0 | 0 | 1 | 0 | 1 |
| 208. | 192.168.1.228 | 0 | 0 | 1 | 0 | 1 |
| 209. | 192.168.1.229 | 0 | 0 | 1 | 0 | 1 |
| 210. | 192.168.1.230 | 0 | 0 | 1 | 0 | 1 |
| 211. | 192.168.1.231 | 0 | 0 | 1 | 0 | 1 |
| 212. | 192.168.1.232 | 0 | 0 | 1 | 0 | 1 |
| 213. | 192.168.1.233 | 0 | 0 | 1 | 0 | 1 |
| 214. | 192.168.1.234 | 0 | 0 | 1 | 0 | 1 |
| 215. | 192.168.1.235 | 0 | 0 | 1 | 0 | 1 |
| 216. | 192.168.1.236 | 0 | 0 | 1 | 0 | 1 |
| 217. | 192.168.1.237 | 0 | 0 | 1 | 0 | 1 |
| 218. | 192.168.1.238 | 0 | 0 | 1 | 0 | 1 |
| 219. | 192.168.1.239 | 0 | 0 | 1 | 0 | 1 |
| 220. | 192.168.1.240 | 0 | 0 | 1 | 0 | 1 |
| 221. | 192.168.1.241 | 0 | 0 | 1 | 0 | 1 |
| 222. | 192.168.1.242 | 0 | 0 | 1 | 0 | 1 |
| 223. | 192.168.1.243 | 0 | 0 | 1 | 0 | 1 |
| 224. | 192.168.1.244 | 0 | 0 | 1 | 0 | 1 |
| 225. | 192.168.1.245 | 0 | 0 | 1 | 0 | 1 |
| 226. | 192.168.1.246 | 0 | 0 | 1 | 0 | 1 |
| 227. | 192.168.1.247 | 0 | 0 | 1 | 0 | 1 |
| 228. | 192.168.1.248 | 3 | 12 | 27 | 0 | 42 |
| 229. | 192.168.1.251 | 0 | 0 | 0 | 0 | 0 |
| 230. | 192.168.1.254 | 0 | 0 | 4 | 0 | 4 |
| Summary | | 21 | 36 | 298 | 8 | 363 |

| * Phase\_2 |
| --- |

| 192.168.2.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.2.61 | 0 | 0 | 2 | 0 | 2 |
| 2. | 192.168.2.62 | 0 | 0 | 1 | 0 | 1 |
| 3. | 192.168.2.63 | 0 | 0 | 2 | 0 | 2 |
| 4. | 192.168.2.64 | 0 | 0 | 2 | 0 | 2 |
| 5. | 192.168.2.65 | 0 | 0 | 2 | 0 | 2 |
| 6. | 192.168.2.66 | 0 | 0 | 2 | 0 | 2 |
| 7. | 192.168.2.67 | 0 | 0 | 2 | 0 | 2 |
| 8. | 192.168.2.68 | 0 | 0 | 2 | 0 | 2 |
| 9. | 192.168.2.69 | 0 | 0 | 2 | 0 | 2 |
| 10. | 192.168.2.70 | 0 | 0 | 2 | 0 | 2 |
| 11. | 192.168.2.71 | 0 | 0 | 2 | 0 | 2 |
| 12. | 192.168.2.72 | 0 | 0 | 2 | 0 | 2 |
| 13. | 192.168.2.73 | 0 | 0 | 2 | 0 | 2 |
| 14. | 192.168.2.81 | 2 | 0 | 0 | 0 | 2 |
| 15. | 192.168.2.82 | 2 | 0 | 0 | 0 | 2 |
| 16. | 192.168.2.83 | 1 | 0 | 0 | 0 | 1 |
| 17. | 192.168.2.84 | 2 | 0 | 0 | 0 | 2 |
| 18. | 192.168.2.85 | 2 | 0 | 0 | 0 | 2 |
| 19. | 192.168.2.86 | 0 | 2 | 17 | 1 | 20 |
| 20. | 192.168.2.87 | 2 | 0 | 0 | 0 | 2 |
| 21. | 192.168.2.88 | 2 | 0 | 0 | 0 | 2 |
| 22. | 192.168.2.89 | 2 | 0 | 0 | 0 | 2 |
| 23. | 192.168.2.90 | 2 | 0 | 0 | 0 | 2 |
| 24. | 192.168.2.91 | 2 | 0 | 0 | 0 | 2 |
| 25. | 192.168.2.92 | 2 | 0 | 0 | 0 | 2 |
| 26. | 192.168.2.93 | 2 | 0 | 0 | 0 | 2 |
| 27. | 192.168.2.94 | 2 | 0 | 0 | 0 | 2 |
| 28. | 192.168.2.95 | 2 | 0 | 0 | 0 | 2 |
| 29. | 192.168.2.96 | 2 | 0 | 0 | 0 | 2 |
| 30. | 192.168.2.97 | 2 | 0 | 0 | 0 | 2 |
| 31. | 192.168.2.98 | 2 | 0 | 0 | 0 | 2 |
| 32. | 192.168.2.99 | 2 | 0 | 0 | 0 | 2 |
| 33. | 192.168.2.102 | 0 | 0 | 0 | 0 | 0 |
| 34. | 192.168.2.103 | 0 | 0 | 0 | 0 | 0 |
| 35. | 192.168.2.104 | 1 | 0 | 0 | 0 | 1 |
| 36. | 192.168.2.105 | 1 | 0 | 0 | 0 | 1 |
| 37. | 192.168.2.106 | 2 | 0 | 0 | 0 | 2 |
| 38. | 192.168.2.107 | 2 | 0 | 0 | 0 | 2 |
| 39. | 192.168.2.108 | 2 | 0 | 0 | 0 | 2 |
| 40. | 192.168.2.109 | 2 | 0 | 0 | 0 | 2 |
| 41. | 192.168.2.110 | 2 | 0 | 0 | 0 | 2 |
| 42. | 192.168.2.111 | 2 | 0 | 0 | 0 | 2 |
| 43. | 192.168.2.112 | 2 | 0 | 0 | 0 | 2 |
| 44. | 192.168.2.113 | 2 | 0 | 0 | 0 | 2 |
| 45. | 192.168.2.114 | 2 | 0 | 0 | 0 | 2 |
| 46. | 192.168.2.115 | 2 | 0 | 0 | 0 | 2 |
| 47. | 192.168.2.116 | 2 | 0 | 0 | 0 | 2 |
| 48. | 192.168.2.117 | 2 | 0 | 0 | 0 | 2 |
| 49. | 192.168.2.118 | 2 | 0 | 0 | 0 | 2 |
| 50. | 192.168.2.119 | 2 | 0 | 0 | 0 | 2 |
| 51. | 192.168.2.120 | 2 | 0 | 0 | 0 | 2 |
| 52. | 192.168.2.121 | 1 | 0 | 0 | 0 | 1 |
| 53. | 192.168.2.122 | 1 | 0 | 0 | 0 | 1 |
| 54. | 192.168.2.123 | 1 | 0 | 0 | 0 | 1 |
| 55. | 192.168.2.124 | 1 | 0 | 0 | 0 | 1 |
| 56. | 192.168.2.125 | 2 | 0 | 0 | 0 | 2 |
| 57. | 192.168.2.126 | 2 | 0 | 0 | 0 | 2 |
| 58. | 192.168.2.127 | 2 | 0 | 0 | 0 | 2 |
| 59. | 192.168.2.128 | 2 | 0 | 0 | 0 | 2 |
| 60. | 192.168.2.129 | 2 | 0 | 0 | 0 | 2 |
| 61. | 192.168.2.130 | 2 | 0 | 0 | 0 | 2 |
| 62. | 192.168.2.131 | 0 | 2 | 17 | 1 | 20 |
| 63. | 192.168.2.132 | 2 | 0 | 0 | 0 | 2 |
| 64. | 192.168.2.133 | 2 | 0 | 0 | 0 | 2 |
| 65. | 192.168.2.134 | 2 | 0 | 0 | 0 | 2 |
| 66. | 192.168.2.135 | 2 | 0 | 0 | 0 | 2 |
| 67. | 192.168.2.136 | 2 | 0 | 0 | 0 | 2 |
| 68. | 192.168.2.137 | 2 | 0 | 0 | 0 | 2 |
| 69. | 192.168.2.138 | 2 | 0 | 0 | 0 | 2 |
| 70. | 192.168.2.139 | 2 | 0 | 0 | 0 | 2 |
| 71. | 192.168.2.140 | 2 | 0 | 0 | 0 | 2 |
| 72. | 192.168.2.141 | 2 | 0 | 0 | 0 | 2 |
| 73. | 192.168.2.142 | 2 | 0 | 0 | 0 | 2 |
| 74. | 192.168.2.143 | 2 | 0 | 0 | 0 | 2 |
| 75. | 192.168.2.144 | 2 | 0 | 0 | 0 | 2 |
| 76. | 192.168.2.145 | 2 | 0 | 0 | 0 | 2 |
| 77. | 192.168.2.146 | 2 | 0 | 0 | 0 | 2 |
| 78. | 192.168.2.147 | 0 | 2 | 17 | 1 | 20 |
| 79. | 192.168.2.148 | 2 | 0 | 0 | 0 | 2 |
| 80. | 192.168.2.149 | 2 | 0 | 0 | 0 | 2 |
| 81. | 192.168.2.150 | 2 | 0 | 0 | 0 | 2 |
| 82. | 192.168.2.151 | 2 | 0 | 0 | 0 | 2 |
| 83. | 192.168.2.152 | 2 | 0 | 0 | 0 | 2 |
| 84. | 192.168.2.153 | 2 | 0 | 0 | 0 | 2 |
| 85. | 192.168.2.154 | 2 | 0 | 0 | 0 | 2 |
| 86. | 192.168.2.155 | 0 | 0 | 0 | 0 | 0 |
| 87. | 192.168.2.156 | 2 | 0 | 0 | 0 | 2 |
| 88. | 192.168.2.157 | 2 | 0 | 0 | 0 | 2 |
| 89. | 192.168.2.158 | 2 | 0 | 0 | 0 | 2 |
| 90. | 192.168.2.159 | 2 | 0 | 0 | 0 | 2 |
| 91. | 192.168.2.160 | 2 | 0 | 0 | 0 | 2 |
| 92. | 192.168.2.161 | 2 | 0 | 0 | 0 | 2 |
| 93. | 192.168.2.162 | 2 | 0 | 0 | 0 | 2 |
| 94. | 192.168.2.163 | 2 | 0 | 0 | 0 | 2 |
| 95. | 192.168.2.164 | 2 | 0 | 0 | 0 | 2 |
| 96. | 192.168.2.165 | 2 | 0 | 0 | 0 | 2 |
| 97. | 192.168.2.166 | 2 | 0 | 0 | 0 | 2 |
| 98. | 192.168.2.167 | 2 | 0 | 0 | 0 | 2 |
| 99. | 192.168.2.168 | 2 | 0 | 0 | 0 | 2 |
| 100. | 192.168.2.169 | 2 | 0 | 0 | 0 | 2 |
| 101. | 192.168.2.170 | 2 | 0 | 0 | 0 | 2 |
| 102. | 192.168.2.171 | 2 | 0 | 0 | 0 | 2 |
| 103. | 192.168.2.172 | 2 | 0 | 0 | 0 | 2 |
| 104. | 192.168.2.173 | 2 | 0 | 0 | 0 | 2 |
| 105. | 192.168.2.174 | 2 | 0 | 0 | 0 | 2 |
| 106. | 192.168.2.175 | 2 | 0 | 0 | 0 | 2 |
| 107. | 192.168.2.176 | 2 | 0 | 0 | 0 | 2 |
| 108. | 192.168.2.177 | 2 | 0 | 0 | 0 | 2 |
| 109. | 192.168.2.178 | 0 | 1 | 8 | 0 | 9 |
| 110. | 192.168.2.179 | 2 | 0 | 0 | 0 | 2 |
| 111. | 192.168.2.180 | 2 | 0 | 0 | 0 | 2 |
| 112. | 192.168.2.181 | 1 | 0 | 0 | 0 | 1 |
| 113. | 192.168.2.182 | 0 | 0 | 0 | 0 | 0 |
| 114. | 192.168.2.183 | 0 | 0 | 0 | 0 | 0 |
| 115. | 192.168.2.184 | 2 | 0 | 0 | 0 | 2 |
| 116. | 192.168.2.186 | 2 | 0 | 0 | 0 | 2 |
| 117. | 192.168.2.187 | 2 | 0 | 0 | 0 | 2 |
| 118. | 192.168.2.188 | 2 | 0 | 0 | 0 | 2 |
| 119. | 192.168.2.189 | 2 | 0 | 0 | 0 | 2 |
| 120. | 192.168.2.190 | 2 | 0 | 0 | 0 | 2 |
| 121. | 192.168.2.191 | 2 | 0 | 0 | 0 | 2 |
| 122. | 192.168.2.192 | 2 | 0 | 0 | 0 | 2 |
| 123. | 192.168.2.193 | 2 | 0 | 0 | 0 | 2 |
| 124. | 192.168.2.194 | 2 | 0 | 0 | 0 | 2 |
| 125. | 192.168.2.195 | 0 | 2 | 17 | 1 | 20 |
| 126. | 192.168.2.196 | 2 | 0 | 0 | 0 | 2 |
| 127. | 192.168.2.197 | 0 | 0 | 0 | 0 | 0 |
| 128. | 192.168.2.198 | 2 | 0 | 0 | 0 | 2 |
| 129. | 192.168.2.199 | 0 | 0 | 0 | 0 | 0 |
| 130. | 192.168.2.200 | 2 | 0 | 0 | 0 | 2 |
| 131. | 192.168.2.201 | 0 | 0 | 0 | 0 | 0 |
| 132. | 192.168.2.202 | 1 | 0 | 0 | 0 | 1 |
| 133. | 192.168.2.203 | 0 | 0 | 0 | 0 | 0 |
| 134. | 192.168.2.204 | 0 | 0 | 0 | 0 | 0 |
| 135. | 192.168.2.205 | 1 | 0 | 0 | 0 | 1 |
| 136. | 192.168.2.206 | 1 | 0 | 0 | 0 | 1 |
| 137. | 192.168.2.207 | 2 | 0 | 0 | 0 | 2 |
| 138. | 192.168.2.208 | 0 | 0 | 0 | 0 | 0 |
| 139. | 192.168.2.209 | 0 | 0 | 0 | 0 | 0 |
| 140. | 192.168.2.210 | 2 | 0 | 0 | 0 | 2 |
| 141. | 192.168.2.211 | 0 | 1 | 8 | 0 | 9 |
| 142. | 192.168.2.212 | 2 | 0 | 0 | 0 | 2 |
| 143. | 192.168.2.213 | 2 | 0 | 0 | 0 | 2 |
| 144. | 192.168.2.214 | 2 | 0 | 0 | 0 | 2 |
| 145. | 192.168.2.215 | 2 | 0 | 0 | 0 | 2 |
| 146. | 192.168.2.216 | 2 | 0 | 0 | 0 | 2 |
| 147. | 192.168.2.217 | 0 | 0 | 20 | 1 | 21 |
| 148. | 192.168.2.218 | 2 | 0 | 0 | 0 | 2 |
| 149. | 192.168.2.219 | 2 | 0 | 0 | 0 | 2 |
| 150. | 192.168.2.220 | 2 | 0 | 0 | 0 | 2 |
| 151. | 192.168.2.221 | 0 | 2 | 17 | 1 | 20 |
| 152. | 192.168.2.222 | 2 | 0 | 0 | 0 | 2 |
| 153. | 192.168.2.223 | 2 | 0 | 0 | 0 | 2 |
| 154. | 192.168.2.224 | 2 | 0 | 0 | 0 | 2 |
| 155. | 192.168.2.225 | 2 | 0 | 0 | 0 | 2 |
| 156. | 192.168.2.226 | 2 | 0 | 0 | 0 | 2 |
| 157. | 192.168.2.227 | 1 | 0 | 1 | 0 | 2 |
| 158. | 192.168.2.228 | 0 | 2 | 17 | 1 | 20 |
| Summary | | 236 | 14 | 164 | 7 | 421 |

| * Phase\_2.1 |
| --- |

| 192.168.3.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.3.2 | 0 | 0 | 0 | 0 | 0 |
| 2. | 192.168.3.3 | 0 | 0 | 0 | 0 | 0 |
| 3. | 192.168.3.4 | 0 | 0 | 0 | 0 | 0 |
| 4. | 192.168.3.5 | 0 | 0 | 0 | 0 | 0 |
| 5. | 192.168.3.6 | 0 | 0 | 0 | 0 | 0 |
| 6. | 192.168.3.7 | 0 | 0 | 0 | 0 | 0 |
| 7. | 192.168.3.8 | 0 | 0 | 0 | 0 | 0 |
| 8. | 192.168.3.10 | 0 | 0 | 0 | 0 | 0 |
| 9. | 192.168.3.13 | 0 | 0 | 0 | 0 | 0 |
| 10. | 192.168.3.14 | 0 | 0 | 0 | 0 | 0 |
| 11. | 192.168.3.15 | 0 | 0 | 0 | 0 | 0 |
| 12. | 192.168.3.16 | 0 | 0 | 0 | 0 | 0 |
| 13. | 192.168.3.17 | 0 | 0 | 0 | 0 | 0 |
| 14. | 192.168.3.18 | 0 | 0 | 0 | 0 | 0 |
| 15. | 192.168.3.22 | 0 | 0 | 1 | 0 | 1 |
| 16. | 192.168.3.23 | 0 | 0 | 1 | 0 | 1 |
| 17. | 192.168.3.25 | 0 | 0 | 1 | 0 | 1 |
| 18. | 192.168.3.26 | 0 | 0 | 1 | 0 | 1 |
| 19. | 192.168.3.27 | 0 | 0 | 1 | 0 | 1 |
| 20. | 192.168.3.28 | 0 | 0 | 1 | 0 | 1 |
| 21. | 192.168.3.29 | 0 | 0 | 1 | 0 | 1 |
| 22. | 192.168.3.30 | 0 | 0 | 1 | 0 | 1 |
| 23. | 192.168.3.31 | 0 | 0 | 1 | 0 | 1 |
| 24. | 192.168.3.32 | 0 | 0 | 1 | 0 | 1 |
| 25. | 192.168.3.33 | 0 | 0 | 1 | 0 | 1 |
| 26. | 192.168.3.34 | 0 | 0 | 1 | 0 | 1 |
| 27. | 192.168.3.35 | 0 | 0 | 1 | 0 | 1 |
| 28. | 192.168.3.36 | 0 | 0 | 1 | 0 | 1 |
| 29. | 192.168.3.37 | 0 | 0 | 1 | 0 | 1 |
| 30. | 192.168.3.38 | 0 | 0 | 1 | 0 | 1 |
| 31. | 192.168.3.39 | 0 | 0 | 1 | 0 | 1 |
| 32. | 192.168.3.40 | 0 | 0 | 1 | 0 | 1 |
| 33. | 192.168.3.41 | 0 | 0 | 1 | 0 | 1 |
| 34. | 192.168.3.42 | 0 | 0 | 1 | 0 | 1 |
| 35. | 192.168.3.43 | 0 | 0 | 1 | 0 | 1 |
| 36. | 192.168.3.44 | 0 | 0 | 1 | 0 | 1 |
| 37. | 192.168.3.45 | 0 | 0 | 1 | 0 | 1 |
| 38. | 192.168.3.46 | 0 | 0 | 1 | 0 | 1 |
| 39. | 192.168.3.47 | 0 | 0 | 1 | 0 | 1 |
| 40. | 192.168.3.48 | 0 | 0 | 1 | 0 | 1 |
| 41. | 192.168.3.49 | 0 | 0 | 1 | 0 | 1 |
| 42. | 192.168.3.50 | 0 | 0 | 1 | 0 | 1 |
| 43. | 192.168.3.51 | 0 | 0 | 1 | 0 | 1 |
| 44. | 192.168.3.52 | 0 | 0 | 1 | 0 | 1 |
| 45. | 192.168.3.53 | 0 | 0 | 1 | 0 | 1 |
| 46. | 192.168.3.55 | 0 | 0 | 1 | 0 | 1 |
| 47. | 192.168.3.56 | 0 | 0 | 1 | 0 | 1 |
| 48. | 192.168.3.57 | 0 | 0 | 1 | 0 | 1 |
| 49. | 192.168.3.58 | 0 | 0 | 1 | 0 | 1 |
| 50. | 192.168.3.59 | 0 | 0 | 1 | 0 | 1 |
| 51. | 192.168.3.60 | 0 | 0 | 3 | 0 | 3 |
| 52. | 192.168.3.61 | 0 | 0 | 1 | 0 | 1 |
| 53. | 192.168.3.62 | 0 | 0 | 1 | 0 | 1 |
| 54. | 192.168.3.63 | 0 | 0 | 1 | 0 | 1 |
| 55. | 192.168.3.64 | 0 | 0 | 1 | 0 | 1 |
| 56. | 192.168.3.65 | 0 | 0 | 1 | 0 | 1 |
| 57. | 192.168.3.66 | 0 | 0 | 1 | 0 | 1 |
| 58. | 192.168.3.67 | 0 | 0 | 1 | 0 | 1 |
| 59. | 192.168.3.68 | 0 | 0 | 1 | 0 | 1 |
| 60. | 192.168.3.69 | 0 | 0 | 1 | 0 | 1 |
| 61. | 192.168.3.70 | 0 | 0 | 1 | 0 | 1 |
| 62. | 192.168.3.71 | 0 | 0 | 1 | 0 | 1 |
| 63. | 192.168.3.72 | 0 | 0 | 1 | 0 | 1 |
| 64. | 192.168.3.73 | 0 | 0 | 1 | 0 | 1 |
| 65. | 192.168.3.74 | 0 | 0 | 1 | 0 | 1 |
| 66. | 192.168.3.75 | 0 | 0 | 1 | 0 | 1 |
| 67. | 192.168.3.80 | 0 | 2 | 1 | 0 | 3 |
| 68. | 192.168.3.87 | 0 | 0 | 0 | 0 | 0 |
| 69. | 192.168.3.89 | 0 | 0 | 0 | 0 | 0 |
| 70. | 192.168.3.90 | 0 | 0 | 0 | 0 | 0 |
| 71. | 192.168.3.91 | 0 | 0 | 0 | 0 | 0 |
| 72. | 192.168.3.92 | 0 | 0 | 0 | 0 | 0 |
| 73. | 192.168.3.93 | 0 | 0 | 0 | 0 | 0 |
| 74. | 192.168.3.94 | 0 | 0 | 0 | 0 | 0 |
| 75. | 192.168.3.95 | 0 | 0 | 0 | 0 | 0 |
| 76. | 192.168.3.96 | 0 | 0 | 0 | 0 | 0 |
| 77. | 192.168.3.103 | 0 | 0 | 0 | 0 | 0 |
| 78. | 192.168.3.104 | 0 | 0 | 0 | 0 | 0 |
| 79. | 192.168.3.108 | 0 | 0 | 0 | 0 | 0 |
| 80. | 192.168.3.117 | 0 | 0 | 2 | 0 | 2 |
| 81. | 192.168.3.118 | 0 | 0 | 2 | 0 | 2 |
| 82. | 192.168.3.119 | 0 | 0 | 2 | 0 | 2 |
| 83. | 192.168.3.120 | 0 | 0 | 4 | 0 | 4 |
| 84. | 192.168.3.121 | 0 | 0 | 4 | 0 | 4 |
| 85. | 192.168.3.122 | 0 | 0 | 4 | 0 | 4 |
| 86. | 192.168.3.123 | 0 | 0 | 2 | 0 | 2 |
| 87. | 192.168.3.124 | 0 | 0 | 2 | 0 | 2 |
| 88. | 192.168.3.127 | 0 | 0 | 4 | 0 | 4 |
| 89. | 192.168.3.128 | 1 | 1 | 6 | 3 | 11 |
| 90. | 192.168.3.129 | 0 | 0 | 4 | 0 | 4 |
| 91. | 192.168.3.130 | 1 | 1 | 6 | 3 | 11 |
| 92. | 192.168.3.131 | 0 | 0 | 4 | 0 | 4 |
| 93. | 192.168.3.132 | 0 | 0 | 4 | 0 | 4 |
| 94. | 192.168.3.133 | 0 | 0 | 2 | 0 | 2 |
| 95. | 192.168.3.134 | 0 | 0 | 4 | 0 | 4 |
| 96. | 192.168.3.161 | 3 | 2 | 11 | 2 | 18 |
| 97. | 192.168.3.162 | 2 | 3 | 10 | 1 | 16 |
| 98. | 192.168.3.163 | 0 | 0 | 6 | 0 | 6 |
| 99. | 192.168.3.170 | 0 | 0 | 0 | 0 | 0 |
| 100. | 192.168.3.172 | 0 | 0 | 0 | 0 | 0 |
| 101. | 192.168.3.173 | 0 | 0 | 0 | 0 | 0 |
| 102. | 192.168.3.210 | 0 | 1 | 2 | 0 | 3 |
| 103. | 192.168.3.220 | 0 | 0 | 4 | 0 | 4 |
| 104. | 192.168.3.222 | 0 | 1 | 2 | 0 | 3 |
| 105. | 192.168.3.223 | 0 | 1 | 2 | 0 | 3 |
| 106. | 192.168.3.224 | 0 | 1 | 2 | 0 | 3 |
| 107. | 192.168.3.225 | 0 | 1 | 2 | 0 | 3 |
| 108. | 192.168.3.226 | 0 | 1 | 1 | 0 | 2 |
| 109. | 192.168.3.227 | 0 | 1 | 2 | 0 | 3 |
| 110. | 192.168.3.228 | 0 | 1 | 2 | 0 | 3 |
| 111. | 192.168.3.229 | 0 | 1 | 2 | 0 | 3 |
| 112. | 192.168.3.230 | 0 | 1 | 2 | 0 | 3 |
| 113. | 192.168.3.231 | 0 | 0 | 4 | 0 | 4 |
| 114. | 192.168.3.232 | 0 | 0 | 4 | 0 | 4 |
| Summary | | 7 | 19 | 169 | 9 | 204 |

| * VM Server |
| --- |

| 192.168.13.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.13.11 | 1 | 1 | 14 | 1 | 17 |
| 2. | 192.168.13.12 | 0 | 0 | 7 | 0 | 7 |
| 3. | 192.168.13.13 | 0 | 0 | 0 | 0 | 0 |
| 4. | 192.168.13.14 | 0 | 0 | 6 | 0 | 6 |
| 5. | 192.168.13.15 | 0 | 0 | 0 | 0 | 0 |
| 6. | 192.168.13.16 | 0 | 0 | 6 | 0 | 6 |
| 7. | 192.168.13.17 | 3 | 12 | 30 | 1 | 46 |
| 8. | 192.168.13.18 | 0 | 0 | 6 | 0 | 6 |
| 9. | 192.168.13.19 | 1 | 0 | 6 | 0 | 7 |
| 10. | 192.168.13.20 | 0 | 1 | 16 | 0 | 17 |
| 11. | 192.168.13.21 | 0 | 0 | 11 | 0 | 11 |
| 12. | 192.168.13.22 | 1 | 1 | 14 | 1 | 17 |
| 13. | 192.168.13.23 | 1 | 1 | 21 | 1 | 24 |
| 14. | 192.168.13.24 | 0 | 0 | 12 | 0 | 12 |
| Summary | | 7 | 16 | 149 | 4 | 176 |



**ตารางที่ 4** แสดงตารางแสดงผลช่องโหว่ COCO-IDC3 All