**รายงานสรุปผลการตรวจสอบช่องโหว่ของระบบ All Dell cloud**

**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 All Dell cloud จำนวน 62 รายการ ที่ บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) อาคารไทยซัมมิททาวเวอร์   
ชั้น 10 ในวันที่ 25 กุมภาพันธ์ 2565 เวลา 19:30 น. – 21:00 น.

# รายงานสรุปผลการตรวจสอบ

รายงานสรุปผลการตรวจสอบนี้ใช้สำหรับผู้ดูแลระบบ การเตรียมความพร้อมในการแก้ไขช่องโหว่ที่ตรวจพบมีจุดประสงค์เพื่อลดความรุนแรงและผลกระทบจากการถูกบุกรุกผ่านช่องโหว่ดังกล่าว จากผลการตรวจสอบสรุปจำนวนช่องโหว่ตามระดับความเสี่ยงจากภายในเครือข่ายของแต่ละเครื่อง/อุปกรณ์ดังตารางด้านล่างนี้

| รายการอุปกรณ์ | จำนวน IP | Critical | High | Medium | Low | Info |
| --- | --- | --- | --- | --- | --- | --- |
| ESXi Host | 35 | 20 | 46 | 153 | 10 | 999 |
| VM Server | 27 | 12 | 23 | 82 | 12 | 739 |
| Summary | 62 | 32 | 69 | 235 | 22 | 1738 |

**ตารางที่ 1** แสดงสรุปรายละเอียดผลการตรวจสอบช่องโหว่ที่ตรวจพบ

## สรุปภาพโดยรวมช่องโหว่ที่ตรวจสอบพบบนระบบ Cloud Dell

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | สรุปภาพรวมในการตรวจสอบช่องโหว่บนระบบ Cloud Dell  โดยมีเครื่องที่ให้บริการและอุปกรณ์เครือข่ายที่ได้รับการตรวจสอบ  ทั้งหมด จำนวน 62 รายการ   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **ระดับความรุนแรง** | **CRITICAL** | **HIGH** | **MED** | **LOW** | | **เปอร์เซ็นต์** | 9% | 19% | 66% | 6% | | **จำนวนช่องโหว่** | 32 | 69 | 235 | 22 | |

**ตารางที่ 2** แสดงภาพรวมช่องโหว่ที่ตรวจพบของระบบ Cloud Dell

## สรุปช่องโหว่พร้อมแนวทางแก้ไขโดยสังเขป

| ลำดับที่ | หมายเลขไอพี | รายละเอียดช่องโหว่ | ระดับความเสี่ยง | คำแนะนำในการแก้ไข |
| --- | --- | --- | --- | --- |
|  | 192.168.8.13 192.168.8.91 192.168.8.160 192.168.8.171 192.168.8.211 192.168.10.27 192.168.10.220 192.168.10.226 192.168.11.160 192.168.11.200 | 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. |
|  | 192.168.10.4 192.168.10.7 | VMware vCenter Server 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2021-0027)  - The version of VMware vCenter Server installed on the remote host is 6.5 prior to 6.5 U3r or 6.7 prior to 6.7 U3p. It is, therefore, affected by multiple vulnerabilities:  - An arbitrary file read vulnerability exists in the vSphere web client. An unauthenticated, remote attacker  can exploit this, via HTTPS, to gain access to sensitive information. (CVE-2021-21980)  - A server side request forgery vulnerability exists in the vSAN Web Client plug-in. An unauthenticated,  remote attacker can exploit this, via HTTPS, to cause the server to access internal services or access  sites outside of vCenter. (CVE-2021-22049) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version  number. Nessus has also not tested for the presence of a workaround. | Critical | * Upgrade to VMware vCenter Server 6.5 U3r, 6.7 U3p, or later. |
|  | 192.168.8.136 192.168.8.166 192.168.8.167 192.168.8.168 192.168.8.231 192.168.8.232 192.168.8.245 192.168.8.246 192.168.10.191 192.168.10.193 192.168.10.194 192.168.11.132 192.168.11.134 192.168.11.141 192.168.11.142 192.168.11.143 192.168.11.144 192.168.11.151 192.168.11.152 192.168.11.153 | ESXi 6.5 / 6.7 XSS (VMSA-2020-0008)  - The remote VMware ESXi host is version 6.5 or 6.7 and is affected by a cross-site scripting (XSS) vulnerability in virtual machine attributes due to improper validation of user-supplied input before returning it to users. An authenticated, remote attacker with access to modify the system properties of a virtual machine from inside the guest OS can exploit this, by inserting script-related HTML in the system properties and having a user view the system properties from the ESXi Host Client, to execute arbitrary script code in a user's ESXi Host Client session. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | Critical | * Apply the appropriate patch as referenced in the vendor advisory. |
|  | 192.168.8.12 192.168.8.13 192.168.8.91 192.168.8.160 192.168.8.171 192.168.8.211 192.168.8.212 192.168.8.213 192.168.10.1 192.168.10.27 192.168.10.220 192.168.10.226 192.168.11.160 192.168.11.200 | 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. | High | * Reconfigure the affected application if possible to avoid use of medium strength ciphers. |
|  | 192.168.8.13 192.168.8.211 192.168.10.27 192.168.10.220 192.168.10.226 | 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. | High | * Contact the Certificate Authority to have the SSL certificate reissued. |
|  | 192.168.8.13 192.168.8.91 192.168.8.160 192.168.8.171 | 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. |
|  | 192.168.8.136 192.168.8.166 192.168.8.167 192.168.8.168 192.168.8.231 192.168.8.232 192.168.8.245 192.168.8.246 192.168.10.191 192.168.10.193 192.168.10.194 192.168.11.132 192.168.11.134 192.168.11.141 192.168.11.142 192.168.11.143 192.168.11.144 192.168.11.151 192.168.11.152 192.168.11.153 | ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)  - According to its self-reported version number, the remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by multiple vulnerabilities.   - A use-after-free error exists in the XHCI USB controller. An unauthenticated, local attacker with local  administrative privileges on a virtual machine can exploit this, to execute code as the virtual machine's  VMX process running on the host. (CVE-2020-4004)  - A privilege escalation vulnerability exists in ESXi due to how certain system calls are managed. An  authenticated, local attacker with privileges within the VPM process can exploit this, when chained with  CVE-2020-4004, to obtain escalated privileges. (CVE-2020-4005) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | High | * Apply the appropriate patch as referenced in the vendor advisory. |
|  | 192.168.8.136 192.168.8.166 192.168.8.167 192.168.8.168 192.168.8.231 192.168.8.232 192.168.8.245 192.168.8.246 192.168.10.191 192.168.10.193 192.168.10.194 | ESXi 6.0 / 6.5 / 6.7 Out-of-Bounds Read Vulnerability (VMSA-2018-0026) (Remote Check)  - The remote VMware ESXi host is version 6.0, 6.5, or 6.7 and is missing a security patch. It is, therefore, vulnerable to an out-of-bounds read vulnerability in SVGA devices. An attacker with access to a guest system may be able to execute code on the host system by leveraging this vulnerability. | High | * Apply the appropriate patch as referenced in the vendor advisory. |
|  | 192.168.8.136 192.168.8.166 192.168.8.167 192.168.8.168 192.168.8.231 192.168.8.232 192.168.8.245 192.168.8.246 192.168.10.191 192.168.10.193 192.168.10.194 | ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2018-0027) (Remote Check)  - The remote VMware ESXi host is version 6.0, 6.5, or 6.7 and is missing a security patch. It is, therefore, vulnerable to multiple vulnerabilities. Leveraging the most severe of these vulnerabilities could allow an attacker to execute arbitrary code on the host from the security context of an unprivileged user on the guest system. Note: CVE-2018-6982 only applies to ESXi 6.5 and 6.7 installations.  ESXi 6.0 installations are not affected. | High | * Apply the appropriate patch as referenced in the vendor advisory. |
|  | 192.168.8.231 192.168.8.232 | ESXi 5.5 / 6.0 / 6.5 / Multiple Vulnerabilities (VMSA-2017-0021) (VMSA-2018-0002) (Spectre) (remote check)  - The remote VMware ESXi host is version 5.5, 6.0, or 6.5 and is missing a security patch. It is, therefore, affected by multiple vulnerabilities that can allow code execution in a virtual machine via the authenticated VNC session as well as cause information disclosure from one virtual machine to another virtual machine on the same host. | High | * Apply the appropriate patch as referenced in the vendor advisory. |
|  | 192.168.8.231 192.168.8.232 | ESXi 6.5 Build 6765664 Heap Buffer Overflow (VMSA-2017-0021) (remote check)  - The version of the remote VMware ESXi 6.5 host is prior to build 6765664. It is, therefore, affected by a heap buffer overflow vulnerability that can be triggered by a specially crafted set of VNC packets. | High | * Apply patch ESXi650-201710401-BG according to the vendor advisory. |
|  | 192.168.8.12 192.168.8.13 192.168.8.15 192.168.8.35 192.168.8.91 192.168.8.136 192.168.8.137 192.168.8.160 192.168.8.166 192.168.8.167 192.168.8.168 192.168.8.171 192.168.8.211 192.168.8.212 192.168.8.213 192.168.8.231 192.168.8.232 192.168.8.245 192.168.8.246 192.168.10.1 192.168.10.4 192.168.10.7 192.168.10.27 192.168.10.191 192.168.10.192 192.168.10.193 192.168.10.194 192.168.10.210 192.168.10.220 192.168.10.226 192.168.11.131 192.168.11.132 192.168.11.134 192.168.11.135 192.168.11.141 192.168.11.142 192.168.11.143 192.168.11.144 192.168.11.151 192.168.11.152 192.168.11.153 192.168.11.160 192.168.11.176 192.168.11.177 192.168.11.178 192.168.11.179 192.168.11.180 192.168.11.181 192.168.11.182 192.168.11.183 192.168.11.184 192.168.11.185 192.168.11.200 | 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. |
|  | 192.168.8.12 192.168.8.13 192.168.8.35 192.168.8.91 192.168.8.136 192.168.8.160 192.168.8.166 192.168.8.167 192.168.8.168 192.168.8.171 192.168.8.211 192.168.8.212 192.168.8.213 192.168.8.231 192.168.8.232 192.168.8.245 192.168.8.246 192.168.10.1 192.168.10.27 192.168.10.191 192.168.10.192 192.168.10.193 192.168.10.194 192.168.10.210 192.168.10.220 192.168.10.226 192.168.11.131 192.168.11.132 192.168.11.134 192.168.11.135 192.168.11.141 192.168.11.142 192.168.11.143 192.168.11.144 192.168.11.151 192.168.11.152 192.168.11.153 192.168.11.160 192.168.11.176 192.168.11.177 192.168.11.178 192.168.11.179 192.168.11.180 192.168.11.181 192.168.11.182 192.168.11.183 192.168.11.184 192.168.11.185 192.168.11.200 | 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. |
|  | 192.168.8.12 192.168.8.13 192.168.8.91 192.168.8.160 192.168.8.171 192.168.8.211 192.168.8.212 192.168.8.213 192.168.10.1 192.168.10.27 192.168.10.220 192.168.10.226 192.168.11.160 192.168.11.200 | 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. |
|  | 192.168.8.12 192.168.8.13 192.168.8.15 192.168.8.35 192.168.8.91 192.168.8.136 192.168.8.137 192.168.8.160 192.168.8.166 192.168.8.167 192.168.8.168 192.168.8.171 192.168.8.211 192.168.8.212 192.168.8.213 192.168.8.231 192.168.8.232 192.168.8.245 192.168.8.246 192.168.10.1 192.168.10.4 192.168.10.27 192.168.10.191 192.168.10.192 192.168.10.193 192.168.10.194 192.168.10.220 192.168.10.226 192.168.11.131 192.168.11.132 192.168.11.134 192.168.11.135 192.168.11.141 192.168.11.142 192.168.11.143 192.168.11.144 192.168.11.151 192.168.11.152 192.168.11.153 192.168.11.160 192.168.11.200 | 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. |
|  | 192.168.8.13 192.168.8.91 192.168.8.160 192.168.8.171 192.168.8.211 192.168.10.27 192.168.10.220 192.168.10.226 192.168.11.160 192.168.11.200 | 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. |
|  | 192.168.8.13 192.168.8.91 192.168.8.160 192.168.8.171 | 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. |
|  | 192.168.8.13 | 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. |
|  | 192.168.8.136 192.168.8.166 192.168.8.167 192.168.8.168 192.168.8.231 192.168.8.232 192.168.8.245 192.168.8.246 192.168.10.191 192.168.10.193 192.168.10.194 192.168.11.132 192.168.11.134 192.168.11.141 192.168.11.142 192.168.11.143 192.168.11.144 192.168.11.151 192.168.11.152 192.168.11.153 | ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0005) (Remote Check)  - The remote VMware ESXi host is version 6.0, 6.5, or 6.7 and is missing a security patch. It is, therefore, vulnerable to multiple vulnerabilities, including:  - An out-of-bounds read/write vulnerability and a Time-of-check  Time-of-use (TOCTOU) vulnerability in the virtual USB 1.1 UHCI  (Universal Host Controller Interface). Exploitation of these  issues requires an attacker to have access to a virtual machine  with a virtual USB controller present. These issues may allow a  guest to execute code on the host. (CVE-2019-5518, CVE-2019-5519) | Medium | * Apply the appropriate patch as referenced in the vendor advisory. |
|  | 192.168.8.136 192.168.8.166 192.168.8.167 192.168.8.168 192.168.8.231 192.168.8.232 192.168.8.245 192.168.8.246 192.168.10.191 192.168.10.193 192.168.10.194 192.168.11.132 192.168.11.134 192.168.11.141 192.168.11.142 192.168.11.143 192.168.11.144 192.168.11.151 192.168.11.152 192.168.11.153 | ESXi 6.5 / 6.7 / 7.0 DoS (VMSA-2020-0018)  - The remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by a denial of service (DoS) vulnerability in the authentication service. An unauthenticated, remote attacker can exploit this issue to exhaust memory resources  resulting in a degradation of performance condition while the attack is sustained. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | Medium | * Apply the appropriate patch as referenced in the vendor advisory. |
|  | 192.168.8.136 192.168.8.166 192.168.8.167 192.168.8.168 192.168.8.231 192.168.8.232 192.168.8.245 192.168.8.246 192.168.10.191 192.168.10.193 192.168.10.194 | ESXi 5.5 / 6.0 / 6.5 / 6.7 Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020) (remote check)  - The remote VMware ESXi host is version 5.5, 6.0, 6.5, or 6.7 and is missing a security patch. It is, therefore, vulnerable to a speculative execution side channel attack known as L1 Terminal Fault (L1TF). An attacker who successfully exploited L1TF may be able to read privileged data across trust boundaries. | Medium | * Apply the appropriate patch as referenced in the vendor advisory. |
|  | 192.168.8.136 192.168.8.166 192.168.8.167 192.168.8.168 192.168.8.231 192.168.8.232 192.168.8.245 192.168.8.246 192.168.10.191 192.168.10.193 192.168.10.194 | VMware ESXi 5.5 / 6.0 / 6.5 / 6.7 DoS (VMSA-2018-0018) (remote check)  - The remote VMware ESXi host is version 5.5, 6.0, 6.5, or 6.7 and is missing a security patch. It is, therefore, vulnerable to a denial of service vulnerability. The vulnerability exists in the RPC handler due to a NULL pointer dereference issue. An authenticated, remote attacker can exploit this issue to cause VMs to stop responding. | Medium | * Apply the appropriate patch as referenced in the vendor advisory. |
|  | 192.168.8.17 | SSH Weak Algorithms Supported  - Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys. | Medium | * Contact the vendor or consult product documentation to remove the weak ciphers. |
|  | 192.168.8.17 192.168.8.136 192.168.8.138 192.168.8.166 192.168.8.167 192.168.8.168 192.168.8.231 192.168.8.232 192.168.8.245 192.168.8.246 192.168.10.221 192.168.10.222 192.168.10.224 192.168.10.225 192.168.11.151 | 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. |
|  | 192.168.8.17 192.168.10.221 192.168.10.222 192.168.10.224 192.168.10.225 | 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. |
|  | 192.168.8.13 | 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. |
|  | 192.168.8.17 | 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. |

**ตารางที่ 3** รายละเอียดช่องโหว่พร้อมแนวทางการแก้ไข

## ภาคผนวก รายละเอียดรายการ IP ที่ดำเนินการตรวจสอบช่องโหว่

| * VM Server |
| --- |

| 192.168.8.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.8.12 | 0 | 1 | 5 | 0 | 6 |
| 2. | 192.168.8.13 | 1 | 5 | 14 | 1 | 21 |
| 3. | 192.168.8.14 | 0 | 0 | 0 | 0 | 0 |
| 4. | 192.168.8.15 | 0 | 0 | 6 | 0 | 6 |
| 5. | 192.168.8.17 | 0 | 0 | 1 | 3 | 4 |
| 6. | 192.168.8.31 | 0 | 0 | 0 | 0 | 0 |
| 7. | 192.168.8.35 | 0 | 0 | 3 | 0 | 3 |
| 8. | 192.168.8.91 | 1 | 3 | 12 | 0 | 16 |
| 9. | 192.168.8.160 | 1 | 3 | 12 | 0 | 16 |
| 10. | 192.168.8.171 | 1 | 3 | 12 | 0 | 16 |
| 11. | 192.168.8.211 | 1 | 3 | 11 | 0 | 15 |
| 12. | 192.168.8.212 | 0 | 1 | 5 | 0 | 6 |
| 13. | 192.168.8.213 | 0 | 1 | 5 | 0 | 6 |
| Summary | | 5 | 20 | 86 | 4 | 115 |

| 192.168.10.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.10.1 | 0 | 1 | 5 | 0 | 6 |
| 2. | 192.168.10.4 | 2 | 0 | 6 | 0 | 8 |
| 3. | 192.168.10.7 | 2 | 0 | 4 | 0 | 6 |
| 4. | 192.168.10.27 | 1 | 3 | 11 | 0 | 15 |
| 5. | 192.168.10.210 | 0 | 0 | 2 | 0 | 2 |
| 6. | 192.168.10.211 | 0 | 0 | 0 | 0 | 0 |
| 7. | 192.168.10.220 | 1 | 3 | 11 | 0 | 15 |
| 8. | 192.168.10.221 | 0 | 0 | 0 | 2 | 2 |
| 9. | 192.168.10.222 | 0 | 0 | 0 | 2 | 2 |
| 10. | 192.168.10.224 | 0 | 0 | 0 | 2 | 2 |
| 11. | 192.168.10.225 | 0 | 0 | 0 | 2 | 2 |
| 12. | 192.168.10.226 | 1 | 3 | 11 | 0 | 15 |
| Summary | | 7 | 10 | 50 | 8 | 75 |

| 192.168.11.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.11.160 | 1 | 2 | 11 | 0 | 14 |
| 2. | 192.168.11.200 | 1 | 2 | 11 | 0 | 14 |
| Summary | | 2 | 4 | 22 | 0 | 28 |

| * ESXi Host |
| --- |

| 192.168.8.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.8.136 | 1 | 5 | 19 | 1 | 26 |
| 2. | 192.168.8.137 | 0 | 0 | 2 | 0 | 2 |
| 3. | 192.168.8.138 | 0 | 0 | 0 | 1 | 1 |
| 4. | 192.168.8.166 | 1 | 5 | 18 | 1 | 25 |
| 5. | 192.168.8.167 | 1 | 5 | 19 | 1 | 26 |
| 6. | 192.168.8.168 | 1 | 5 | 19 | 1 | 26 |
| 7. | 192.168.8.231 | 1 | 10 | 19 | 1 | 31 |
| 8. | 192.168.8.232 | 1 | 10 | 19 | 1 | 31 |
| 9. | 192.168.8.245 | 1 | 5 | 19 | 1 | 26 |
| 10. | 192.168.8.246 | 1 | 5 | 19 | 1 | 26 |
| Summary | | 8 | 50 | 153 | 9 | 220 |

| 192.168.10.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.10.191 | 1 | 5 | 13 | 0 | 19 |
| 2. | 192.168.10.192 | 0 | 0 | 3 | 0 | 3 |
| 3. | 192.168.10.193 | 1 | 5 | 19 | 0 | 25 |
| 4. | 192.168.10.194 | 1 | 5 | 19 | 0 | 25 |
| Summary | | 3 | 15 | 54 | 0 | 72 |

| 192.168.11.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.11.131 | 0 | 0 | 3 | 0 | 3 |
| 2. | 192.168.11.132 | 1 | 2 | 17 | 0 | 20 |
| 3. | 192.168.11.134 | 1 | 2 | 17 | 0 | 20 |
| 4. | 192.168.11.135 | 0 | 0 | 5 | 0 | 5 |
| 5. | 192.168.11.141 | 1 | 2 | 17 | 0 | 20 |
| 6. | 192.168.11.142 | 1 | 2 | 17 | 0 | 20 |
| 7. | 192.168.11.143 | 1 | 2 | 17 | 0 | 20 |
| 8. | 192.168.11.144 | 1 | 2 | 17 | 0 | 20 |
| 9. | 192.168.11.151 | 1 | 2 | 12 | 1 | 16 |
| 10. | 192.168.11.152 | 1 | 2 | 17 | 0 | 20 |
| 11. | 192.168.11.153 | 1 | 2 | 17 | 0 | 20 |
| 12. | 192.168.11.176 | 0 | 0 | 7 | 0 | 7 |
| 13. | 192.168.11.177 | 0 | 0 | 5 | 0 | 5 |
| 14. | 192.168.11.178 | 0 | 0 | 7 | 0 | 7 |
| 15. | 192.168.11.179 | 0 | 0 | 5 | 0 | 5 |
| 16. | 192.168.11.180 | 0 | 0 | 7 | 0 | 7 |
| 17. | 192.168.11.181 | 0 | 0 | 2 | 0 | 2 |
| 18. | 192.168.11.182 | 0 | 0 | 7 | 0 | 7 |
| 19. | 192.168.11.183 | 0 | 0 | 7 | 0 | 7 |
| 20. | 192.168.11.184 | 0 | 0 | 7 | 0 | 7 |
| 21. | 192.168.11.185 | 0 | 0 | 7 | 0 | 7 |
| Summary | | 9 | 18 | 217 | 1 | 245 |



**ตารางที่ 5** แสดงตารางแสดงผลช่องโหว่ ESXi Host Dell Cloud