**รายงานสรุปผลการตรวจสอบช่องโหว่ของระบบ Cloud Dell**

**บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) ประจำปี 2564**

# 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 Cloud Dell จำนวน 165 รายการ ที่ บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) อาคารไทยซัมมิททาวเวอร์   
ชั้น 10 ในวันที่ 11 กุมภาพันธ์ 2564 เวลา 19:30 น. – 21:00 น.

# รายงานสรุปผลการตรวจสอบ

รายงานสรุปผลการตรวจสอบนี้ใช้สำหรับผู้ดูแลระบบ การเตรียมความพร้อมในการแก้ไขช่องโหว่ที่ตรวจพบมีจุดประสงค์เพื่อลดความรุนแรงและผลกระทบจากการถูกบุกรุกผ่านช่องโหว่ดังกล่าว จากผลการตรวจสอบสรุปจำนวนช่องโหว่ตามระดับความเสี่ยงจากภายในเครือข่ายของแต่ละเครื่อง/อุปกรณ์ดังตารางด้านล่างนี้

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| รายการอุปกรณ์ | จำนวน IP | Critical | High | Medium | Low | Info |
| VMware Dell Cloud | 30 | 5 | 0 | 134 | 7 | 813 |
| ESXi Host Dell Cloud | 35 | 0 | 85 | 204 | 24 | 988 |
| Summary | 65 | 5 | 85 | 338 | 31 | 1801 |

**ตารางที่ 1** แสดงสรุปรายละเอียดผลการตรวจสอบช่องโหว่ที่ตรวจพบ

## สรุปภาพโดยรวมช่องโหว่ที่ตรวจสอบพบบนระบบ Cloud Dell

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | สรุปภาพรวมในการตรวจสอบช่องโหว่บนระบบ Cloud Dell  โดยมีเครื่องที่ให้บริการและอุปกรณ์เครือข่ายที่ได้รับการตรวจสอบ  ทั้งหมด จำนวน 65 รายการ   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **ระดับความรุนแรง** | **CRITICAL** | **HIGH** | **MED** | **LOW** | | **เปอร์เซ็นต์** | 1% | 18% | 74% | 7% | | **จำนวนช่องโหว่** | 5 | 85 | 338 | 31 | |

**ตารางที่ 2** แสดงภาพรวมช่องโหว่ที่ตรวจพบของระบบ Cloud Dell

## สรุปช่องโหว่พร้อมแนวทางแก้ไขโดยสังเขป

| ลำดับที่ | หมายเลขไอพี | รายละเอียดช่องโหว่ | ระดับความเสี่ยง | คำแนะนำในการแก้ไข |
| --- | --- | --- | --- | --- |
|  | 192.168.8.91  192.168.8.160  192.168.8.171  192.168.10.220  192.168.10.226 | Microsoft SQL Server Unsupported Version Detection  ตรวจพบว่ามีการใช้งานซอฟแวร์ Microsoft SQL Server Version เก่าซึ่งทางผู้พัฒนาได้หยุดการสนับสนุนซอฟแวร์ Version ดังกล่าวแล้ว ส่งผลให้ไม่มีการแก้ไขหรือพัฒนาต่อรวมไปถึงการแก้ไขช่องโหว่บนซอฟแวร์ | **Critical** | * Upgrade ให้เป็น Version ปัจจุบัน |
|  | 192.168.8.13  192.168.8.91  192.168.8.160  192.168.8.171 | อุปกรณ์มีการใช้งาน SSL 2.0 และ SSL 3.0 โดยทั้งสอง Version มีจุดอ่อนในการเข้ารหัส ทำให้ผู้โจมตีมีโอกาสที่จะสามารถทำการถอดรหัสข้อมูลได้ | **High** | * ทำการ Disable SSL 2.0 และ SSL 3.0 แล้วเปลี่ยนมาใช้ TLS 1.2 แทน |
|  | 192.168.8.136  192.168.8.137  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  192.168.10.191  192.168.10.193  192.168.10.194  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 | อุปกรณ์มีการใช้งาน VMware ESXi version 6.0, 6.5, และ 6.7 ซึ่งเป็น Version ที่มีหลายช่องโหว่เช่น   * An out-of-bounds read/write vulnerability and Time-of-check-Time-of-use (TOCTOU) vulnerability ใน virtual USB 1.1 UHCI | **High** | * ทำการ Update Patch ตามที่ผู้ให้บริการแนะนำ |
|  | 192.168.8.136  192.168.8.137  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  192.168.10.191  192.168.10.193  192.168.10.194 | อุปกรณ์มีการใช้งาน VMware ESXi version 6.0, 6.5, และ 6.7 ซึ่งเป็น Version ที่มีหลายช่องโหว่เช่น   * ผู้โจมตีสามารถใช้งานค่ำสั่งนอกเหนือจากสิทธิ์ของ user บน Guest OS ได้   CVE-2018-6982 | **High** | * ทำการ Update Patch ตามที่ผู้ให้บริการแนะนำ |
|  | 192.168.8.136  192.168.8.137  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  192.168.10.191  192.168.10.193  192.168.10.194 | อุปกรณ์มีการใช้งาน VMware ESXi version 6.0, 6.5, และ 6.7 ซึ่งเป็น Version ที่มีหลายช่องโหว่เช่น   * An out-of-bounds read vulnerabilitiy in SVGA Devices ผู้โจมตีที่เข้าถึง Guest OS สามารถใช้งานคำสั่งบน Host OS ได้ | **High** | * ทำการ Update Patch ตามที่ผู้ให้บริการแนะนำ |
|  | 192.168.8.136  192.168.8.137  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  192.168.10.191  192.168.10.192  192.168.10.193  192.168.10.194  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  192.168.11.176  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 | อุปกรณ์มีการใช้งาน VMware ESXi version 6.5, 6.7, และ 7.0 ซึ่งเป็น Version ที่มีหลายช่องโหว่เช่น   * CVE-2020-4004 * CVE-2020-4005 | **High** | * ทำการUpdate Path เป็น Version ล่าสุด |

**ตารางที่ 3** รายละเอียดช่องโหว่พร้อมแนวทางการแก้ไข

## ภาคผนวก รายละเอียดรายการ IP ที่ดำเนินการตรวจสอบช่องโหว่

* **VMware Dell Cloud**

| 192.168.8.x | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 192.168.8.12 | 0 | 0 | 0 | 0 | 0 |
|  | 192.168.8.13 | 0 | 1 | 10 | 1 | 12 |
|  | 192.168.8.14 | 0 | 0 | 3 | 0 | 3 |
|  | 192.168.8.15 | 0 | 0 | 6 | 0 | 6 |
|  | 192.168.8.17 | 0 | 0 | 1 | 2 | 3 |
|  | 192.168.8.31 | 0 | 0 | 3 | 0 | 3 |
|  | 192.168.8.35 | 0 | 0 | 3 | 0 | 3 |
|  | 192.168.8.91 | 1 | 1 | 7 | 0 | 9 |
|  | 192.168.8.160 | 1 | 1 | 7 | 0 | 9 |
|  | 192.168.8.171 | 1 | 1 | 7 | 0 | 9 |
|  | 192.168.8.211 | 0 | 0 | 8 | 0 | 8 |
|  | 192.168.8.212 | 0 | 0 | 5 | 0 | 5 |
|  | 192.168.8.213 | 0 | 0 | 5 | 0 | 5 |
| Summary | | 3 | 4 | 55 | 3 | 65 |

| 192.168.10.x | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 192.168.10.1 | 0 | 0 | 6 | 0 | 6 |
|  | 192.168.10.4 | 0 | 0 | 2 | 0 | 2 |
|  | 192.168.10.7 | 0 | 0 | 4 | 0 | 4 |
|  | 192.168.10.27 | 0 | 0 | 8 | 0 | 8 |
|  | 192.168.10.28 | 0 | 0 | 5 | 0 | 5 |
|  | 192.168.10.29 | 0 | 0 | 5 | 0 | 5 |
|  | 192.168.10.210 | 0 | 0 | 2 | 0 | 2 |
|  | 192.168.10.211 | 0 | 0 | 2 | 0 | 2 |
|  | 192.168.10.220 | 1 | 0 | 8 | 0 | 9 |
|  | 192.168.10.221 | 0 | 0 | 0 | 1 | 1 |
|  | 192.168.10.222 | 0 | 0 | 0 | 1 | 1 |
|  | 192.168.10.224 | 0 | 0 | 0 | 1 | 1 |
|  | 192.168.10.225 | 0 | 0 | 0 | 1 | 1 |
|  | 192.168.10.226 | 1 | 0 | 8 | 0 | 9 |
| Summary | | 2 | 0 | 50 | 4 | 56 |

| 192.168.11.x | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 192.168.11.160 | 0 | 0 | 6 | 0 | 6 |
|  | 192.168.11.199 | 0 | 0 | 7 | 0 | 7 |
|  | 192.168.11.200 | 0 | 0 | 6 | 0 | 6 |
| Summary | | 0 | 0 | 19 | 0 | 19 |

**ตารางที่ 4** แสดงตารางแสดงผลช่องโหว่ VMware Dell Cloud

* **ESXi Host Dell Cloud**

| 192.168.8.x | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 192.168.8.136 | 0 | 4 | 7 | 1 | 12 |
|  | 192.168.8.137 | 0 | 4 | 7 | 0 | 11 |
|  | 192.168.8.138 | 0 | 4 | 7 | 1 | 12 |
|  | 192.168.8.166 | 0 | 4 | 7 | 0 | 11 |
|  | 192.168.8.167 | 0 | 4 | 7 | 0 | 11 |
|  | 192.168.8.168 | 0 | 4 | 7 | 1 | 12 |
|  | 192.168.8.231 | 0 | 4 | 9 | 1 | 14 |
|  | 192.168.8.232 | 0 | 4 | 9 | 1 | 14 |
|  | 192.168.8.245 | 0 | 4 | 7 | 1 | 12 |
|  | 192.168.8.246 | 0 | 4 | 7 | 1 | 12 |
| Summary | | 0 | 40 | 74 | 7 | 121 |

| 192.168.10.x | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 192.168.10.191 | 0 | 4 | 7 | 1 | 12 |
|  | 192.168.10.192 | 0 | 1 | 4 | 1 | 6 |
|  | 192.168.10.193 | 0 | 4 | 7 | 1 | 12 |
|  | 192.168.10.194 | 0 | 4 | 7 | 1 | 12 |
| Summary | | 0 | 13 | 25 | 4 | 42 |

| 192.168.11.x | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 192.168.11.131 | 0 | 2 | 5 | 1 | 8 |
|  | 192.168.11.132 | 0 | 2 | 5 | 0 | 7 |
|  | 192.168.11.134 | 0 | 2 | 5 | 0 | 7 |
|  | 192.168.11.135 | 0 | 2 | 5 | 0 | 7 |
|  | 192.168.11.141 | 0 | 2 | 5 | 1 | 8 |
|  | 192.168.11.142 | 0 | 2 | 5 | 1 | 8 |
|  | 192.168.11.143 | 0 | 2 | 5 | 1 | 8 |
|  | 192.168.11.144 | 0 | 2 | 5 | 1 | 8 |
|  | 192.168.11.151 | 0 | 2 | 5 | 1 | 8 |
|  | 192.168.11.152 | 0 | 2 | 5 | 0 | 7 |
|  | 192.168.11.153 | 0 | 2 | 5 | 1 | 8 |
|  | 192.168.11.176 | 0 | 1 | 5 | 1 | 7 |
|  | 192.168.11.177 | 0 | 1 | 5 | 1 | 7 |
|  | 192.168.11.178 | 0 | 1 | 5 | 1 | 7 |
|  | 192.168.11.179 | 0 | 1 | 5 | 1 | 7 |
|  | 192.168.11.180 | 0 | 1 | 5 | 1 | 7 |
|  | 192.168.11.181 | 0 | 1 | 5 | 0 | 6 |
|  | 192.168.11.182 | 0 | 1 | 5 | 0 | 6 |
|  | 192.168.11.183 | 0 | 1 | 5 | 0 | 6 |
|  | 192.168.11.184 | 0 | 1 | 5 | 0 | 6 |
|  | 192.168.11.185 | 0 | 1 | 5 | 1 | 7 |
| Summary | | 0 | 32 | 105 | 13 | 150 |

**ตารางที่ 5** แสดงตารางแสดงผลช่องโหว่ ESXi Host Dell Cloud