**รายงานสรุปผลการตรวจสอบช่องโหว่ของระบบ**

**บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) ประจำปี**

# 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 จำนวน 165 รายการ ที่ บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) อาคารไทยซัมมิททาวเวอร์   
ชั้น 10 ในวันที่ 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 |
| --- | --- | --- | --- | --- |

**ตารางที่ 3** รายละเอียดช่องโหว่พร้อมแนวทางการแก้ไข

## ภาคผนวก รายละเอียดรายการ IP ที่ดำเนินการตรวจสอบช่องโหว่

* **VMware Dell Cloud**



| 10.20.121.x | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 10.20.121.20 | 0 | 1 | 5 | 0 | 6 |
|  | 10.20.121.200 | 0 | 0 | 1 | 0 | 1 |
|  | 10.20.121.210 | 0 | 1 | 6 | 3 | 10 |
|  | 10.20.121.245 | 0 | 0 | 0 | 0 | 0 |
|  | 10.90.210.235 | 0 | 0 | 3 | 0 | 3 |
|  | 10.100.10.136 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.138 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.139 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.140 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.143 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.183 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.184 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.185 | 0 | 0 | 3 | 0 | 3 |
|  | 10.100.10.186 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.188 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.189 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.191 | 1 | 5 | 8 | 1 | 15 |
|  | 10.100.10.192 | 0 | 3 | 4 | 0 | 7 |
| Summary | | 11 | 60 | 110 | 4 | 185 |

| 10.100.10.x | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 10.20.121.20 | 0 | 1 | 5 | 0 | 6 |
|  | 10.20.121.200 | 0 | 0 | 1 | 0 | 1 |
|  | 10.20.121.210 | 0 | 1 | 6 | 3 | 10 |
|  | 10.20.121.245 | 0 | 0 | 0 | 0 | 0 |
|  | 10.90.210.235 | 0 | 0 | 3 | 0 | 3 |
|  | 10.100.10.136 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.138 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.139 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.140 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.143 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.183 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.184 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.185 | 0 | 0 | 3 | 0 | 3 |
|  | 10.100.10.186 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.188 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.189 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.191 | 1 | 5 | 8 | 1 | 15 |
|  | 10.100.10.192 | 0 | 3 | 4 | 0 | 7 |
| Summary | | 11 | 60 | 110 | 4 | 185 |

| 10.90.210.x | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 10.20.121.20 | 0 | 1 | 5 | 0 | 6 |
|  | 10.20.121.200 | 0 | 0 | 1 | 0 | 1 |
|  | 10.20.121.210 | 0 | 1 | 6 | 3 | 10 |
|  | 10.20.121.245 | 0 | 0 | 0 | 0 | 0 |
|  | 10.90.210.235 | 0 | 0 | 3 | 0 | 3 |
|  | 10.100.10.136 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.138 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.139 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.140 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.143 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.183 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.184 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.185 | 0 | 0 | 3 | 0 | 3 |
|  | 10.100.10.186 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.188 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.189 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.191 | 1 | 5 | 8 | 1 | 15 |
|  | 10.100.10.192 | 0 | 3 | 4 | 0 | 7 |
| Summary | | 11 | 60 | 110 | 4 | 185 |

**ตารางที่ 5** แสดงตารางแสดงผลช่องโหว่ ESXi Host Dell Cloud