**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.xxx | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 10.20.121.20 | 0 | 1 | 5 | 0 | 6 |
|  | 10.20.121.200 | 0 | 0 | 3 | 0 | 3 |
|  | 10.20.121.210 | 0 | 1 | 6 | 3 | 10 |
|  | 10.20.121.245 | 0 | 0 | 3 | 0 | 3 |
| Summary | | 0 | 2 | 17 | 3 | 22 |

| 10.20.33.xxx | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 10.20.33.180 | 0 | 0 | 3 | 0 | 3 |
|  | 10.20.33.199 | 0 | 0 | 3 | 3 | 6 |
|  | 10.20.33.210 | 0 | 0 | 0 | 0 | 0 |
|  | 10.20.33.235 | 0 | 0 | 0 | 0 | 0 |
|  | 10.20.33.245 | 0 | 1 | 6 | 0 | 7 |
| Summary | | 0 | 1 | 12 | 3 | 16 |

| 10.20.80.xxx | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 10.20.80.10 | 9 | 7 | 21 | 4 | 41 |
|  | 10.20.80.21 | 0 | 0 | 0 | 0 | 0 |
|  | 10.20.80.22 | 0 | 0 | 0 | 0 | 0 |
|  | 10.20.80.23 | 0 | 0 | 0 | 0 | 0 |
|  | 10.20.80.35 | 0 | 0 | 0 | 0 | 0 |
|  | 10.20.80.41 | 2 | 6 | 5 | 0 | 13 |
|  | 10.20.80.50 | 2 | 4 | 5 | 2 | 13 |
|  | 10.20.80.53 | 2 | 4 | 5 | 0 | 11 |
|  | 10.20.80.57 | 2 | 6 | 5 | 0 | 13 |
|  | 10.20.80.58 | 2 | 0 | 2 | 0 | 4 |
|  | 10.20.80.59 | 2 | 0 | 2 | 0 | 4 |
|  | 10.20.80.60 | 2 | 6 | 5 | 0 | 13 |
|  | 10.20.80.63 | 2 | 6 | 5 | 0 | 13 |
|  | 10.20.80.64 | 2 | 6 | 5 | 0 | 13 |
|  | 10.20.80.65 | 2 | 0 | 4 | 1 | 7 |
|  | 10.20.80.68 | 2 | 0 | 4 | 0 | 6 |
|  | 10.20.80.69 | 2 | 6 | 5 | 0 | 13 |
|  | 10.20.80.70 | 2 | 6 | 5 | 0 | 13 |
|  | 10.20.80.71 | 2 | 6 | 5 | 0 | 13 |
|  | 10.20.80.74 | 1 | 2 | 6 | 1 | 10 |
|  | 10.20.80.76 | 2 | 4 | 5 | 0 | 11 |
|  | 10.20.80.77 | 0 | 0 | 1 | 0 | 1 |
|  | 10.20.80.78 | 2 | 4 | 5 | 0 | 11 |
|  | 10.20.80.81 | 2 | 0 | 4 | 0 | 6 |
|  | 10.20.80.82 | 2 | 4 | 5 | 0 | 11 |
|  | 10.20.80.83 | 2 | 4 | 5 | 0 | 11 |
|  | 10.20.80.84 | 2 | 0 | 8 | 0 | 10 |
|  | 10.20.80.85 | 2 | 0 | 4 | 0 | 6 |
|  | 10.20.80.91 | 1 | 2 | 6 | 0 | 9 |
|  | 10.20.80.141 | 2 | 6 | 5 | 2 | 15 |
|  | 10.20.80.145 | 2 | 0 | 8 | 0 | 10 |
|  | 10.20.80.151 | 2 | 4 | 5 | 0 | 11 |
|  | 10.20.80.161 | 2 | 0 | 2 | 0 | 4 |
|  | 10.20.80.162 | 2 | 4 | 5 | 0 | 11 |
|  | 10.20.80.165 | 2 | 0 | 4 | 0 | 6 |
|  | 10.20.80.166 | 2 | 4 | 5 | 0 | 11 |
|  | 10.20.80.171 | 2 | 6 | 5 | 0 | 13 |
|  | 10.20.80.172 | 1 | 2 | 6 | 0 | 9 |
|  | 10.20.80.173 | 1 | 2 | 6 | 0 | 9 |
|  | 10.20.80.186 | 2 | 0 | 8 | 0 | 10 |
| Summary | | 73 | 111 | 191 | 10 | 385 |

| 10.20.90.xxx | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 10.20.90.8 | 0 | 0 | 1 | 0 | 1 |
|  | 10.20.90.52 | 0 | 0 | 0 | 0 | 0 |
|  | 10.20.90.53 | 0 | 0 | 0 | 0 | 0 |
|  | 10.20.90.56 | 0 | 0 | 1 | 3 | 4 |
|  | 10.20.90.58 | 1 | 4 | 12 | 1 | 18 |
| Summary | | 1 | 4 | 14 | 4 | 23 |

| 10.90.10.xxx | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 10.90.10.8 | 0 | 0 | 6 | 0 | 6 |
|  | 10.90.10.9 | 1 | 17 | 7 | 1 | 26 |
|  | 10.90.10.10 | 0 | 0 | 5 | 0 | 5 |
|  | 10.90.10.19 | 0 | 1 | 6 | 0 | 7 |
|  | 10.90.10.44 | 1 | 3 | 6 | 0 | 10 |
|  | 10.90.10.45 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.10.111 | 1 | 3 | 7 | 1 | 12 |
|  | 10.90.10.112 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.10.113 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.10.181 | 1 | 3 | 7 | 0 | 11 |
|  | 10.90.10.182 | 1 | 3 | 9 | 1 | 14 |
|  | 10.90.10.183 | 1 | 3 | 7 | 0 | 11 |
|  | 10.90.10.185 | 1 | 3 | 6 | 0 | 10 |
| Summary | | 10 | 87 | 87 | 3 | 187 |

| 10.90.20.xxx | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 10.90.20.8 | 0 | 14 | 3 | 0 | 17 |
|  | 10.90.20.9 | 1 | 19 | 12 | 2 | 34 |
|  | 10.90.20.10 | 0 | 14 | 3 | 0 | 17 |
|  | 10.90.20.19 | 0 | 1 | 6 | 0 | 7 |
|  | 10.90.20.20 | 0 | 0 | 0 | 0 | 0 |
|  | 10.90.20.39 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.40 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.41 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.42 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.43 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.44 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.45 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.46 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.47 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.48 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.111 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.112 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.113 | 1 | 3 | 7 | 1 | 12 |
|  | 10.90.20.114 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.115 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.116 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.117 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.118 | 1 | 18 | 9 | 2 | 30 |
|  | 10.90.20.119 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.121 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.124 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.125 | 1 | 3 | 7 | 0 | 11 |
|  | 10.90.20.126 | 1 | 3 | 7 | 0 | 11 |
|  | 10.90.20.181 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.20.182 | 1 | 17 | 7 | 0 | 25 |
| Summary | | 26 | 432 | 201 | 5 | 664 |

| 10.90.30.xxx | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 10.90.30.8 | 0 | 0 | 3 | 0 | 3 |
|  | 10.90.30.9 | 1 | 17 | 6 | 1 | 25 |
|  | 10.90.30.10 | 0 | 0 | 1 | 0 | 1 |
|  | 10.90.30.19 | 0 | 0 | 0 | 0 | 0 |
|  | 10.90.30.20 | 0 | 0 | 0 | 0 | 0 |
|  | 10.90.30.50 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.30.114 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.30.144 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.30.150 | 1 | 18 | 9 | 2 | 30 |
| Summary | | 5 | 86 | 40 | 3 | 134 |

| 10.100.10.xxx | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 10.100.10.10 | 0 | 1 | 6 | 0 | 7 |
|  | 10.100.10.131 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.132 | 1 | 5 | 8 | 1 | 15 |
|  | 10.100.10.133 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.134 | 1 | 2 | 4 | 0 | 7 |
|  | 10.100.10.135 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.136 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.137 | 1 | 5 | 8 | 1 | 15 |
|  | 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 |
|  | 10.100.10.180 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.181 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.182 | 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 |
|  | 10.100.10.187 | 1 | 5 | 8 | 1 | 15 |
|  | 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 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.193 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.194 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.195 | 1 | 5 | 8 | 0 | 14 |
|  | 10.100.10.196 | 1 | 5 | 8 | 0 | 14 |
| Summary | | 26 | 128 | 213 | 4 | 371 |

| 10.90.40.xxx | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 10.90.40.8 | 0 | 14 | 1 | 0 | 15 |
|  | 10.90.40.9 | 1 | 3 | 8 | 1 | 13 |
|  | 10.90.40.10 | 1 | 3 | 14 | 1 | 19 |
|  | 10.90.40.19 | 0 | 1 | 6 | 0 | 7 |
|  | 10.90.40.20 | 0 | 0 | 1 | 0 | 1 |
|  | 10.90.40.111 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.40.122 | 1 | 3 | 7 | 0 | 11 |
|  | 10.90.40.133 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.40.181 | 1 | 17 | 7 | 0 | 25 |
|  | 10.90.40.183 | 1 | 17 | 7 | 0 | 25 |
| Summary | | 7 | 92 | 65 | 2 | 166 |

| 10.100.40.xxx | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 10.100.40.151 | 1 | 2 | 6 | 1 | 10 |
| Summary | | 1 | 2 | 6 | 1 | 10 |

| 10.90.210.xxx | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
|  | 10.90.210.225 | 0 | 0 | 3 | 0 | 3 |
|  | 10.90.210.235 | 0 | 0 | 3 | 0 | 3 |
| Summary | | 0 | 0 | 6 | 0 | 6 |

**ตารางที่ 5** แสดงตารางแสดงผลช่องโหว่ ESXi Host Dell Cloud