**รายงานสรุปผลการตรวจสอบช่องโหว่ของระบบ COCO-IDC1 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-IDC1 All จำนวน 69 รายการ ที่ บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) อาคารไทยซัมมิททาวเวอร์ ชั้น 10 ในวันที่ 03 มีนาคม 2565 เวลา 19:30 น. – 21:00 น.

# รายงานสรุปผลการตรวจสอบ

รายงานสรุปผลการตรวจสอบนี้ใช้สำหรับผู้ดูแลระบบ การเตรียมความพร้อมในการแก้ไขช่องโหว่ที่ตรวจพบมีจุดประสงค์เพื่อลดความรุนแรงและผลกระทบจากการถูกบุกรุกผ่านช่องโหว่ดังกล่าว จากผลการตรวจสอบสรุปจำนวนช่องโหว่ตามระดับความเสี่ยงจากภายในเครือข่ายของแต่ละเครื่อง/อุปกรณ์ดังตารางด้านล่างนี้

| รายการอุปกรณ์ | จำนวน IP | Critical | High | Medium | Low | Info |
| --- | --- | --- | --- | --- | --- | --- |
| CCTV2 Switch POE 24 Port | 15 | 0 | 0 | 0 | 0 | 74 |
| CCTV1 Switch POE 24 Port | 14 | 0 | 0 | 0 | 0 | 68 |
| Server EMS | 1 | 0 | 0 | 0 | 0 | 22 |
| ACC Switch | 9 | 0 | 0 | 0 | 0 | 19 |
| CCTV1 Switch POE 16 Port | 13 | 0 | 0 | 0 | 0 | 41 |
| CCTV2 Switch POE 16 Port | 13 | 0 | 0 | 0 | 0 | 40 |
| VM Backup NVR1, NVR | 1 | 0 | 0 | 0 | 0 | 18 |
| VM Backup EMS | 1 | 0 | 0 | 0 | 0 | 18 |
| ICOM Switch | 2 | 0 | 0 | 0 | 0 | 7 |
| Summary | 69 | 0 | 0 | 0 | 0 | 307 |

**ตารางที่ 1** แสดงสรุปรายละเอียดผลการตรวจสอบช่องโหว่ที่ตรวจพบ

## สรุปภาพโดยรวมช่องโหว่ที่ตรวจสอบพบบนระบบ COCO-IDC1 All

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | สรุปภาพรวมในการตรวจสอบช่องโหว่บนระบบ COCO-IDC1 All  โดยมีเครื่องที่ให้บริการและอุปกรณ์เครือข่ายที่ได้รับการตรวจสอบ  ทั้งหมด จำนวน 69 รายการ   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **ระดับความรุนแรง** | **CRITICAL** | **HIGH** | **MED** | **LOW** | | **เปอร์เซ็นต์** | 0% | 0% | 0% | 0% | | **จำนวนช่องโหว่** | 0 | 0 | 0 | 0 | |

**ตารางที่ 2** แสดงภาพรวมช่องโหว่ที่ตรวจพบของระบบ Cloud Dell

## สรุปช่องโหว่พร้อมแนวทางแก้ไขโดยสังเขป

| ลำดับที่ | หมายเลขไอพี | รายละเอียดช่องโหว่ | ระดับความเสี่ยง | คำแนะนำในการแก้ไข |
| --- | --- | --- | --- | --- |

**ตารางที่ 3** รายละเอียดช่องโหว่พร้อมแนวทางการแก้ไข

## ภาคผนวก รายละเอียดรายการ IP ที่ดำเนินการตรวจสอบช่องโหว่

| * CCTV2 Switch POE 24 Port |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.16 | 0 | 0 | 0 | 0 | 0 |
| 2. | 192.168.12.17 | 0 | 0 | 0 | 0 | 0 |
| 3. | 192.168.12.18 | 0 | 0 | 0 | 0 | 0 |
| 4. | 192.168.12.19 | 0 | 0 | 0 | 0 | 0 |
| 5. | 192.168.12.20 | 0 | 0 | 0 | 0 | 0 |
| 6. | 192.168.12.21 | 0 | 0 | 0 | 0 | 0 |
| 7. | 192.168.12.22 | 0 | 0 | 0 | 0 | 0 |
| 8. | 192.168.12.23 | 0 | 0 | 0 | 0 | 0 |
| 9. | 192.168.12.24 | 0 | 0 | 0 | 0 | 0 |
| 10. | 192.168.12.25 | 0 | 0 | 0 | 0 | 0 |
| 11. | 192.168.12.26 | 0 | 0 | 0 | 0 | 0 |
| 12. | 192.168.12.27 | 0 | 0 | 0 | 0 | 0 |
| 13. | 192.168.12.28 | 0 | 0 | 0 | 0 | 0 |
| 14. | 192.168.12.29 | 0 | 0 | 0 | 0 | 0 |
| 15. | 192.168.12.30 | 0 | 0 | 0 | 0 | 0 |
| Summary | | 0 | 0 | 0 | 0 | 0 |

| * CCTV1 Switch POE 24 Port |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.1 | 0 | 0 | 0 | 0 | 0 |
| 2. | 192.168.12.2 | 0 | 0 | 0 | 0 | 0 |
| 3. | 192.168.12.3 | 0 | 0 | 0 | 0 | 0 |
| 4. | 192.168.12.5 | 0 | 0 | 0 | 0 | 0 |
| 5. | 192.168.12.6 | 0 | 0 | 0 | 0 | 0 |
| 6. | 192.168.12.7 | 0 | 0 | 0 | 0 | 0 |
| 7. | 192.168.12.8 | 0 | 0 | 0 | 0 | 0 |
| 8. | 192.168.12.9 | 0 | 0 | 0 | 0 | 0 |
| 9. | 192.168.12.10 | 0 | 0 | 0 | 0 | 0 |
| 10. | 192.168.12.11 | 0 | 0 | 0 | 0 | 0 |
| 11. | 192.168.12.12 | 0 | 0 | 0 | 0 | 0 |
| 12. | 192.168.12.13 | 0 | 0 | 0 | 0 | 0 |
| 13. | 192.168.12.14 | 0 | 0 | 0 | 0 | 0 |
| 14. | 192.168.12.15 | 0 | 0 | 0 | 0 | 0 |
| Summary | | 0 | 0 | 0 | 0 | 0 |

| * Server EMS |
| --- |

| 192.168.9.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.9.103 | 0 | 0 | 0 | 0 | 0 |
| Summary | | 0 | 0 | 0 | 0 | 0 |

| * ACC Switch |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.73 | 0 | 0 | 0 | 0 | 0 |
| 2. | 192.168.12.76 | 0 | 0 | 0 | 0 | 0 |
| 3. | 192.168.12.78 | 0 | 0 | 0 | 0 | 0 |
| 4. | 192.168.12.79 | 0 | 0 | 0 | 0 | 0 |
| 5. | 192.168.12.82 | 0 | 0 | 0 | 0 | 0 |
| 6. | 192.168.12.84 | 0 | 0 | 0 | 0 | 0 |
| 7. | 192.168.12.87 | 0 | 0 | 0 | 0 | 0 |
| 8. | 192.168.12.90 | 0 | 0 | 0 | 0 | 0 |
| 9. | 192.168.12.94 | 0 | 0 | 0 | 0 | 0 |
| Summary | | 0 | 0 | 0 | 0 | 0 |

| * CCTV1 Switch POE 16 Port |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.4 | 0 | 0 | 0 | 0 | 0 |
| 2. | 192.168.12.31 | 0 | 0 | 0 | 0 | 0 |
| 3. | 192.168.12.32 | 0 | 0 | 0 | 0 | 0 |
| 4. | 192.168.12.33 | 0 | 0 | 0 | 0 | 0 |
| 5. | 192.168.12.34 | 0 | 0 | 0 | 0 | 0 |
| 6. | 192.168.12.35 | 0 | 0 | 0 | 0 | 0 |
| 7. | 192.168.12.36 | 0 | 0 | 0 | 0 | 0 |
| 8. | 192.168.12.37 | 0 | 0 | 0 | 0 | 0 |
| 9. | 192.168.12.38 | 0 | 0 | 0 | 0 | 0 |
| 10. | 192.168.12.39 | 0 | 0 | 0 | 0 | 0 |
| 11. | 192.168.12.40 | 0 | 0 | 0 | 0 | 0 |
| 12. | 192.168.12.41 | 0 | 0 | 0 | 0 | 0 |
| 13. | 192.168.12.42 | 0 | 0 | 0 | 0 | 0 |
| Summary | | 0 | 0 | 0 | 0 | 0 |

| * CCTV2 Switch POE 16 Port |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.43 | 0 | 0 | 0 | 0 | 0 |
| 2. | 192.168.12.44 | 0 | 0 | 0 | 0 | 0 |
| 3. | 192.168.12.45 | 0 | 0 | 0 | 0 | 0 |
| 4. | 192.168.12.46 | 0 | 0 | 0 | 0 | 0 |
| 5. | 192.168.12.47 | 0 | 0 | 0 | 0 | 0 |
| 6. | 192.168.12.48 | 0 | 0 | 0 | 0 | 0 |
| 7. | 192.168.12.49 | 0 | 0 | 0 | 0 | 0 |
| 8. | 192.168.12.50 | 0 | 0 | 0 | 0 | 0 |
| 9. | 192.168.12.51 | 0 | 0 | 0 | 0 | 0 |
| 10. | 192.168.12.52 | 0 | 0 | 0 | 0 | 0 |
| 11. | 192.168.12.54 | 0 | 0 | 0 | 0 | 0 |
| 12. | 192.168.12.55 | 0 | 0 | 0 | 0 | 0 |
| 13. | 192.168.12.56 | 0 | 0 | 0 | 0 | 0 |
| Summary | | 0 | 0 | 0 | 0 | 0 |

| * VM Backup NVR1, NVR |
| --- |

| 192.168.9.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.9.102 | 0 | 0 | 0 | 0 | 0 |
| Summary | | 0 | 0 | 0 | 0 | 0 |

| * VM Backup EMS |
| --- |

| 192.168.9.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.9.101 | 0 | 0 | 0 | 0 | 0 |
| Summary | | 0 | 0 | 0 | 0 | 0 |

| * ICOM Switch |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.103 | 0 | 0 | 0 | 0 | 0 |
| 2. | 192.168.12.104 | 0 | 0 | 0 | 0 | 0 |
| Summary | | 0 | 0 | 0 | 0 | 0 |



**ตารางที่ 4** แสดงตารางแสดงผลช่องโหว่ COCO-IDC1 All