**รายงานสรุปผลการตรวจสอบช่องโหว่ของระบบ COCO-IDC1**

**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 จำนวน 120 รายการ ที่ บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) อาคารไทยซัมมิททาวเวอร์ ชั้น 10 ในวันที่ 12 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 Phase 1 | 15 | 16 | 1 | 28 | 0 | 283 |
| ICOM Switch Phase 1 | 16 | 0 | 0 | 9 | 0 | 141 |
| CCTV2 Switch POE 16 Port Phase 2 | 11 | 20 | 1 | 0 | 0 | 228 |
| ACC Switch Phase 1 | 19 | 0 | 0 | 0 | 0 | 91 |
| etc. | 2 | 2 | 1 | 0 | 0 | 38 |
| PAC Switch Phase 2 | 7 | 0 | 0 | 3 | 0 | 73 |
| VM Backup NVR1 NVR2 | 1 | 0 | 0 | 0 | 0 | 32 |
| ACC Switch Phase 2 | 18 | 0 | 0 | 0 | 0 | 82 |
| CCTV1 Switch Phase 1 | 15 | 17 | 0 | 21 | 1 | 274 |
| Server EMS | 1 | 0 | 0 | 0 | 0 | 30 |
| CCTV1 Switch POE 16 Port Phase 2 | 12 | 24 | 0 | 0 | 0 | 252 |
| VM Backup EMS | 1 | 1 | 0 | 0 | 0 | 34 |
| NVR1 | 1 | 1 | 0 | 0 | 0 | 11 |
| NVR2 | 1 | 0 | 0 | 0 | 0 | 11 |
| Summary | 120 | 81 | 3 | 61 | 1 | 1580 |

**ตารางที่ 1** แสดงสรุปรายละเอียดผลการตรวจสอบช่องโหว่ที่ตรวจพบ

## สรุปภาพโดยรวมช่องโหว่ที่ตรวจสอบพบบนระบบ COCO-IDC1

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | สรุปภาพรวมในการตรวจสอบช่องโหว่บนระบบ COCO-IDC1  โดยมีเครื่องที่ให้บริการและอุปกรณ์เครือข่ายที่ได้รับการตรวจสอบ  ทั้งหมด จำนวน 120 รายการ   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **ระดับความรุนแรง** | **CRITICAL** | **HIGH** | **MED** | **LOW** | | **เปอร์เซ็นต์** | 55.48% | 2.05% | 41.78% | 0.68% | | **จำนวนช่องโหว่** | 81 | 3 | 61 | 1 | |

**ตารางที่ 2** แสดงภาพรวมช่องโหว่ที่ตรวจพบของระบบ Cloud Dell

## สรุปช่องโหว่พร้อมแนวทางแก้ไขโดยสังเขป

| ลำดับที่ | หมายเลขไอพี | รายละเอียดช่องโหว่ | ระดับความเสี่ยง | คำแนะนำในการแก้ไข |
| --- | --- | --- | --- | --- |
|  | 192.168.12.1 192.168.12.3 192.168.12.4 192.168.12.5 192.168.12.6 192.168.12.7 192.168.12.8 192.168.12.9 192.168.12.10 192.168.12.11 192.168.12.12 192.168.12.13 192.168.12.14 192.168.12.15 192.168.12.16 192.168.12.18 192.168.12.19 192.168.12.20 192.168.12.21 192.168.12.22 192.168.12.23 192.168.12.24 192.168.12.25 192.168.12.26 192.168.12.27 192.168.12.28 192.168.12.29 192.168.12.30 | Portable SDK for UPnP Devices (libupnp) 1.6.18 Multiple Stack-based Buffer Overflows RCE  - According to its banner, the version of Portable SDK for UPnP Devices (libupnp) running on the remote host is prior to 1.6.18. It is, therefore, affected by multiple remote code execution vulnerabilities :   - A stack-based buffer overflow condition exists in the  unique\_service\_name() function within file  ssdp/ssdp\_server.c when handling Simple Service  Discovery Protocol (SSDP) requests that is triggered  while copying the DeviceType URN. An unauthenticated,  remote attacker can exploit this, via a specially  crafted SSDP request, to execute arbitrary code.  (CVE-2012-5958)   - A stack-based buffer overflow condition exists in the  unique\_service\_name() function within file  ssdp/ssdp\_server.c when handling Simple Service  Discovery Protocol (SSDP) requests that is triggered  while copying the UDN prior to two colons. An  unauthenticated, remote attacker can exploit this, via a  specially crafted SSDP request, to execute arbitrary  code. (CVE-2012-5959)   - A stack-based buffer overflow condition exists in the  unique\_service\_name() function within file  ssdp/ssdp\_server.c when handling Simple Service  Discovery Protocol (SSDP) requests that is triggered  while copying the UDN prior to the '::upnp:rootdevice'  string. An unauthenticated, remote attacker can exploit  this, via a specially crafted SSDP request, to execute  arbitrary code. (CVE-2012-5960)   - Multiple stack-based buffer overflow conditions exist in  the unique\_service\_name() function within file  ssdp/ssdp\_server.c due to improper validation of the  UDN, DeviceType, and ServiceType fields when parsing  Simple Service Discovery Protocol (SSDP) requests. An  unauthenticated, remote attacker can exploit these  issues, via a specially crafted SSDP request, to execute  arbitrary code. (CVE-2012-5961, CVE-2012-5962,  CVE-2012-5963, CVE-2012-5964, CVE-2012-5965) | **Critical** | * Upgrade to libupnp version 1.6.18 or later. If libupnp is used as a third party library by a different application, contact the vendor of that application for a fix. |
|  | 192.168.12.144 | MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)  - A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.  Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely. | **Critical** | * Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2. |
|  | 192.168.12.2 192.168.12.31 192.168.12.32 192.168.12.33 192.168.12.34 192.168.12.35 192.168.12.36 192.168.12.37 192.168.12.38 192.168.12.39 192.168.12.40 192.168.12.41 192.168.12.42 192.168.12.43 192.168.12.44 192.168.12.45 192.168.12.46 192.168.12.47 192.168.12.48 192.168.12.49 192.168.12.50 192.168.12.51 192.168.12.52 192.168.12.56 | MiniUPnP 1.4 Multiple Vulnerabilities  - According to its banner, the version of MiniUPnP running on the remote host is prior to 1.4. It is, therefore, affected by the following vulnerabilities :   - An out-of-bounds read error exists in the  ProcessSSDPRequest() function in file minissdp.c that  allows an unauthenticated, remote attacker to cause a  denial of service condition via a specially crafted  M-SEARCH request. (CVE-2013-0229)   - A stack-based buffer overflow condition exists in the  ExecuteSoapAction() function in the SOAPAction handler,  due to improper validation of user-supplied input. An  unauthenticated, remote attacker can exploit this, via a  long quoted method, to cause a denial of service  condition or the execution of arbitrary code.  (CVE-2013-0230) | **Critical** | * Upgrade to MiniUPnP version 1.4 or later. |
|  | 192.168.9.101 | Unsupported Windows OS (remote)  - The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities. | **Critical** | * Upgrade to a supported service pack or operating system |
|  | 192.168.12.17 192.168.12.54 192.168.12.55 | Hikvision IP Camera Remote Authentication Bypass  - The remote Hikvision IP camera is affected by an authentication bypass vulnerability. A remote, unauthenticated attacker can read configurations (including account passwords), access the camera images, or modify the camera firmware. | **High** | * Upgrade to a resolved firmware version as per the vendor advisory. |
|  | 192.168.12.1 192.168.12.3 192.168.12.4 192.168.12.5 192.168.12.6 192.168.12.7 192.168.12.8 192.168.12.9 192.168.12.10 192.168.12.11 192.168.12.12 192.168.12.13 192.168.12.14 192.168.12.15 192.168.12.16 192.168.12.18 192.168.12.19 192.168.12.20 192.168.12.21 192.168.12.22 192.168.12.23 192.168.12.24 192.168.12.25 192.168.12.26 192.168.12.27 192.168.12.28 192.168.12.29 192.168.12.30 192.168.12.108 192.168.12.109 | IP Forwarding Enabled  - The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.  Unless the remote host is a router, it is recommended that you disable IP forwarding. | **Medium** | * On Linux, you can disable IP forwarding by doing :  echo 0 > /proc/sys/net/ipv4/ip\_forward  On Windows, set the key 'IPEnableRouter' to 0 under  HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters  On Mac OS X, you can disable IP forwarding by executing the command :  sysctl -w net.inet.ip.forwarding=0  For other systems, check with your vendor. |
|  | 192.168.12.9 192.168.12.10 192.168.12.11 192.168.12.12 192.168.12.13 192.168.12.14 192.168.12.15 192.168.12.16 192.168.12.18 192.168.12.19 192.168.12.20 192.168.12.21 192.168.12.22 192.168.12.23 192.168.12.24 192.168.12.25 192.168.12.26 192.168.12.27 192.168.12.28 192.168.12.29 192.168.12.30 | Unencrypted Telnet Server  - The remote host is running a Telnet server over an unencrypted channel.  Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a  remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.  SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session. | **Medium** | * Disable the Telnet service and use SSH instead. |
|  | 192.168.12.112 192.168.12.113 192.168.12.115 192.168.12.116 192.168.12.118 192.168.12.119 192.168.12.120 192.168.12.122 192.168.12.125 192.168.12.127 | TFTP Traversal Arbitrary File Access  - The TFTP (Trivial File Transfer Protocol) server running on the remote host is vulnerable to a directory traversal attack that allows an attacker to read arbitrary files on the remote host by prepending their names with directory traversal sequences. | **Medium** | * Disable the remote TFTP daemon, run it in a chrooted environment, or filter incoming traffic to this port. |
|  | 192.168.12.15 | SMTP Service Cleartext Login Permitted  - The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used. | **Low** | * Configure the service to support less secure authentication mechanisms only over an encrypted channel. |

**ตารางที่ 3** รายละเอียดช่องโหว่พร้อมแนวทางการแก้ไข

## ภาคผนวก รายละเอียดรายการ IP ที่ดำเนินการตรวจสอบช่องโหว่

| * CCTV2 Switch POE 24 Port Phase 1 |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.16 | 1 | 0 | 2 | 0 | 3 |
| 2. | 192.168.12.17 | 0 | 1 | 0 | 0 | 1 |
| 3. | 192.168.12.18 | 1 | 0 | 2 | 0 | 3 |
| 4. | 192.168.12.19 | 1 | 0 | 2 | 0 | 3 |
| 5. | 192.168.12.20 | 1 | 0 | 2 | 0 | 3 |
| 6. | 192.168.12.21 | 1 | 0 | 2 | 0 | 3 |
| 7. | 192.168.12.22 | 1 | 0 | 2 | 0 | 3 |
| 8. | 192.168.12.23 | 1 | 0 | 2 | 0 | 3 |
| 9. | 192.168.12.24 | 1 | 0 | 2 | 0 | 3 |
| 10. | 192.168.12.25 | 1 | 0 | 2 | 0 | 3 |
| 11. | 192.168.12.26 | 1 | 0 | 2 | 0 | 3 |
| 12. | 192.168.12.27 | 1 | 0 | 2 | 0 | 3 |
| 13. | 192.168.12.28 | 2 | 0 | 2 | 0 | 4 |
| 14. | 192.168.12.29 | 1 | 0 | 2 | 0 | 3 |
| 15. | 192.168.12.30 | 2 | 0 | 2 | 0 | 4 |
| Summary | | 16 | 1 | 28 | 0 | 45 |

| * ICOM Switch Phase 1 |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.102 | 0 | 0 | 0 | 0 | 0 |
| 2. | 192.168.12.103 | 0 | 0 | 0 | 0 | 0 |
| 3. | 192.168.12.104 | 0 | 0 | 0 | 0 | 0 |
| 4. | 192.168.12.105 | 0 | 0 | 0 | 0 | 0 |
| 5. | 192.168.12.106 | 0 | 0 | 0 | 0 | 0 |
| 6. | 192.168.12.108 | 0 | 0 | 1 | 0 | 1 |
| 7. | 192.168.12.109 | 0 | 0 | 1 | 0 | 1 |
| 8. | 192.168.12.112 | 0 | 0 | 1 | 0 | 1 |
| 9. | 192.168.12.113 | 0 | 0 | 1 | 0 | 1 |
| 10. | 192.168.12.114 | 0 | 0 | 0 | 0 | 0 |
| 11. | 192.168.12.115 | 0 | 0 | 1 | 0 | 1 |
| 12. | 192.168.12.116 | 0 | 0 | 1 | 0 | 1 |
| 13. | 192.168.12.117 | 0 | 0 | 0 | 0 | 0 |
| 14. | 192.168.12.118 | 0 | 0 | 1 | 0 | 1 |
| 15. | 192.168.12.119 | 0 | 0 | 1 | 0 | 1 |
| 16. | 192.168.12.120 | 0 | 0 | 1 | 0 | 1 |
| Summary | | 0 | 0 | 9 | 0 | 9 |

| * CCTV2 Switch POE 16 Port Phase 2 |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.43 | 2 | 0 | 0 | 0 | 2 |
| 2. | 192.168.12.44 | 2 | 0 | 0 | 0 | 2 |
| 3. | 192.168.12.45 | 2 | 0 | 0 | 0 | 2 |
| 4. | 192.168.12.46 | 2 | 0 | 0 | 0 | 2 |
| 5. | 192.168.12.47 | 2 | 0 | 0 | 0 | 2 |
| 6. | 192.168.12.48 | 2 | 0 | 0 | 0 | 2 |
| 7. | 192.168.12.49 | 2 | 0 | 0 | 0 | 2 |
| 8. | 192.168.12.50 | 2 | 0 | 0 | 0 | 2 |
| 9. | 192.168.12.51 | 2 | 0 | 0 | 0 | 2 |
| 10. | 192.168.12.52 | 2 | 0 | 0 | 0 | 2 |
| 11. | 192.168.12.54 | 0 | 1 | 0 | 0 | 1 |
| Summary | | 20 | 1 | 0 | 0 | 21 |

| * ACC Switch Phase 1 |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.61 | 0 | 0 | 0 | 0 | 0 |
| 2. | 192.168.12.62 | 0 | 0 | 0 | 0 | 0 |
| 3. | 192.168.12.63 | 0 | 0 | 0 | 0 | 0 |
| 4. | 192.168.12.64 | 0 | 0 | 0 | 0 | 0 |
| 5. | 192.168.12.65 | 0 | 0 | 0 | 0 | 0 |
| 6. | 192.168.12.66 | 0 | 0 | 0 | 0 | 0 |
| 7. | 192.168.12.67 | 0 | 0 | 0 | 0 | 0 |
| 8. | 192.168.12.68 | 0 | 0 | 0 | 0 | 0 |
| 9. | 192.168.12.69 | 0 | 0 | 0 | 0 | 0 |
| 10. | 192.168.12.70 | 0 | 0 | 0 | 0 | 0 |
| 11. | 192.168.12.71 | 0 | 0 | 0 | 0 | 0 |
| 12. | 192.168.12.73 | 0 | 0 | 0 | 0 | 0 |
| 13. | 192.168.12.74 | 0 | 0 | 0 | 0 | 0 |
| 14. | 192.168.12.75 | 0 | 0 | 0 | 0 | 0 |
| 15. | 192.168.12.76 | 0 | 0 | 0 | 0 | 0 |
| 16. | 192.168.12.77 | 0 | 0 | 0 | 0 | 0 |
| 17. | 192.168.12.78 | 0 | 0 | 0 | 0 | 0 |
| 18. | 192.168.12.79 | 0 | 0 | 0 | 0 | 0 |
| 19. | 192.168.12.80 | 0 | 0 | 0 | 0 | 0 |
| Summary | | 0 | 0 | 0 | 0 | 0 |

| * etc. |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.55 | 0 | 1 | 0 | 0 | 1 |
| 2. | 192.168.12.56 | 2 | 0 | 0 | 0 | 2 |
| Summary | | 2 | 1 | 0 | 0 | 3 |

| * PAC Switch Phase 2 |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.121 | 0 | 0 | 0 | 0 | 0 |
| 2. | 192.168.12.122 | 0 | 0 | 1 | 0 | 1 |
| 3. | 192.168.12.123 | 0 | 0 | 0 | 0 | 0 |
| 4. | 192.168.12.124 | 0 | 0 | 0 | 0 | 0 |
| 5. | 192.168.12.125 | 0 | 0 | 1 | 0 | 1 |
| 6. | 192.168.12.126 | 0 | 0 | 0 | 0 | 0 |
| 7. | 192.168.12.127 | 0 | 0 | 1 | 0 | 1 |
| Summary | | 0 | 0 | 3 | 0 | 3 |

| * VM Backup NVR1 NVR2 |
| --- |

| 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 |

| * ACC Switch Phase 2 |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.81 | 0 | 0 | 0 | 0 | 0 |
| 2. | 192.168.12.82 | 0 | 0 | 0 | 0 | 0 |
| 3. | 192.168.12.83 | 0 | 0 | 0 | 0 | 0 |
| 4. | 192.168.12.84 | 0 | 0 | 0 | 0 | 0 |
| 5. | 192.168.12.85 | 0 | 0 | 0 | 0 | 0 |
| 6. | 192.168.12.86 | 0 | 0 | 0 | 0 | 0 |
| 7. | 192.168.12.87 | 0 | 0 | 0 | 0 | 0 |
| 8. | 192.168.12.88 | 0 | 0 | 0 | 0 | 0 |
| 9. | 192.168.12.89 | 0 | 0 | 0 | 0 | 0 |
| 10. | 192.168.12.90 | 0 | 0 | 0 | 0 | 0 |
| 11. | 192.168.12.91 | 0 | 0 | 0 | 0 | 0 |
| 12. | 192.168.12.92 | 0 | 0 | 0 | 0 | 0 |
| 13. | 192.168.12.93 | 0 | 0 | 0 | 0 | 0 |
| 14. | 192.168.12.94 | 0 | 0 | 0 | 0 | 0 |
| 15. | 192.168.12.95 | 0 | 0 | 0 | 0 | 0 |
| 16. | 192.168.12.96 | 0 | 0 | 0 | 0 | 0 |
| 17. | 192.168.12.97 | 0 | 0 | 0 | 0 | 0 |
| 18. | 192.168.12.98 | 0 | 0 | 0 | 0 | 0 |
| Summary | | 0 | 0 | 0 | 0 | 0 |

| * CCTV1 Switch Phase 1 |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.1 | 1 | 0 | 1 | 0 | 2 |
| 2. | 192.168.12.2 | 2 | 0 | 0 | 0 | 2 |
| 3. | 192.168.12.3 | 1 | 0 | 1 | 0 | 2 |
| 4. | 192.168.12.4 | 1 | 0 | 1 | 0 | 2 |
| 5. | 192.168.12.5 | 1 | 0 | 1 | 0 | 2 |
| 6. | 192.168.12.6 | 1 | 0 | 1 | 0 | 2 |
| 7. | 192.168.12.7 | 1 | 0 | 1 | 0 | 2 |
| 8. | 192.168.12.8 | 1 | 0 | 1 | 0 | 2 |
| 9. | 192.168.12.9 | 1 | 0 | 2 | 0 | 3 |
| 10. | 192.168.12.10 | 1 | 0 | 2 | 0 | 3 |
| 11. | 192.168.12.11 | 1 | 0 | 2 | 0 | 3 |
| 12. | 192.168.12.12 | 1 | 0 | 2 | 0 | 3 |
| 13. | 192.168.12.13 | 1 | 0 | 2 | 0 | 3 |
| 14. | 192.168.12.14 | 1 | 0 | 2 | 0 | 3 |
| 15. | 192.168.12.15 | 2 | 0 | 2 | 1 | 5 |
| Summary | | 17 | 0 | 21 | 1 | 39 |

| * 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 |

| * CCTV1 Switch POE 16 Port Phase 2 |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.31 | 2 | 0 | 0 | 0 | 2 |
| 2. | 192.168.12.32 | 2 | 0 | 0 | 0 | 2 |
| 3. | 192.168.12.33 | 2 | 0 | 0 | 0 | 2 |
| 4. | 192.168.12.34 | 2 | 0 | 0 | 0 | 2 |
| 5. | 192.168.12.35 | 2 | 0 | 0 | 0 | 2 |
| 6. | 192.168.12.36 | 2 | 0 | 0 | 0 | 2 |
| 7. | 192.168.12.37 | 2 | 0 | 0 | 0 | 2 |
| 8. | 192.168.12.38 | 2 | 0 | 0 | 0 | 2 |
| 9. | 192.168.12.39 | 2 | 0 | 0 | 0 | 2 |
| 10. | 192.168.12.40 | 2 | 0 | 0 | 0 | 2 |
| 11. | 192.168.12.41 | 2 | 0 | 0 | 0 | 2 |
| 12. | 192.168.12.42 | 2 | 0 | 0 | 0 | 2 |
| Summary | | 24 | 0 | 0 | 0 | 24 |

| * VM Backup EMS |
| --- |

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

| * NVR1 |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.144 | 1 | 0 | 0 | 0 | 1 |
| Summary | | 1 | 0 | 0 | 0 | 1 |

| * NVR2 |
| --- |

| 192.168.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 192.168.12.145 | 0 | 0 | 0 | 0 | 0 |
| Summary | | 0 | 0 | 0 | 0 | 0 |



**ตารางที่ 4** แสดงตารางแสดงผลช่องโหว่ COCO-IDC1