**รายงานสรุปผลการตรวจสอบช่องโหว่ของระบบ Network Cloud**

**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 Network Cloud จำนวน 8 รายการ ที่ บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) อาคารไทยซัมมิททาวเวอร์ ชั้น 10 ในวันที่ 25 กุมภาพันธ์ 2565 เวลา 19:30 น. – 21:00 น.

# รายงานสรุปผลการตรวจสอบ

รายงานสรุปผลการตรวจสอบนี้ใช้สำหรับผู้ดูแลระบบ การเตรียมความพร้อมในการแก้ไขช่องโหว่ที่ตรวจพบมีจุดประสงค์เพื่อลดความรุนแรงและผลกระทบจากการถูกบุกรุกผ่านช่องโหว่ดังกล่าว จากผลการตรวจสอบสรุปจำนวนช่องโหว่ตามระดับความเสี่ยงจากภายในเครือข่ายของแต่ละเครื่อง/อุปกรณ์ดังตารางด้านล่างนี้

| รายการอุปกรณ์ | จำนวน IP | Critical | High | Medium | Low | Info |
| --- | --- | --- | --- | --- | --- | --- |
| Network Group | 8 | 1 | 5 | 13 | 7 | 125 |
| Summary | 8 | 1 | 5 | 13 | 7 | 125 |

**ตารางที่ 1** แสดงสรุปรายละเอียดผลการตรวจสอบช่องโหว่ที่ตรวจพบ

## สรุปภาพโดยรวมช่องโหว่ที่ตรวจสอบพบบนระบบ Network Cloud

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | สรุปภาพรวมในการตรวจสอบช่องโหว่บนระบบ Network Cloud  โดยมีเครื่องที่ให้บริการและอุปกรณ์เครือข่ายที่ได้รับการตรวจสอบ  ทั้งหมด จำนวน 8 รายการ   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **ระดับความรุนแรง** | **CRITICAL** | **HIGH** | **MED** | **LOW** | | **เปอร์เซ็นต์** | 4% | 19% | 50% | 27% | | **จำนวนช่องโหว่** | 1 | 5 | 13 | 7 | |

**ตารางที่ 2** แสดงภาพรวมช่องโหว่ที่ตรวจพบของระบบ Cloud Dell

## สรุปช่องโหว่พร้อมแนวทางแก้ไขโดยสังเขป

| ลำดับที่ | หมายเลขไอพี | รายละเอียดช่องโหว่ | ระดับความเสี่ยง | คำแนะนำในการแก้ไข |
| --- | --- | --- | --- | --- |
|  | 10.11.30.1 | Cisco Application Policy Infrastructure Controller Arbitrary File Read and Write (cisco-sa-capic-frw-Nt3RYxR2)  - According to its self-reported version, Cisco Application Policy Infrastructure Controller is affected by a  vulnerability in an API endpoint which could allow a remote, unauthenticated attacker to read or write  arbitrary files on an affected system.  Please see the included Cisco BIDs and Cisco Security Advisory for more information.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported  version number. | **Critical** | * Upgrade to the relevant fixed version referenced in Cisco bug ID CSCvw57556 |
|  | 10.11.12.123 | SSL Medium Strength Cipher Suites Supported (SWEET32)  - The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or  else that uses the 3DES encryption suite.  Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network. | **High** | * Reconfigure the affected application if possible to avoid use of medium strength ciphers. |
|  | 10.11.30.1 | Cisco Application Policy Infrastructure Controller Linux Kernel IP Fragment Reassembly DoS  - According to its self-reported version, the Cisco Application Policy Infrastructure Controller (APIC) is affected by a vulnerability in the IP stack that is used by the Linux Kernel publicly known as FragmentSmack.  The vulnerability could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. An attack could be executed by an attacker who can submit a stream of fragmented IPv4 or IPv6 packets that are designed to trigger the issue on an affected device. | **High** | * Upgrade to Cisco Application Policy Infrastructure Controller to 3.2.4 / 4.0. |
|  | 10.11.30.1 | Cisco Application Policy Infrastructure Controller REST API Privilege Escalation Vulnerability  - According to its self-reported version, Cisco Application Policy Infrastructure Controller (APIC) is affected by a privilege escalation vulnerability in the REST API. An authenticated, remote attacker could exploit this, via a malicious software upload using the REST API, to gain root access to the system.  Please see the included Cisco BIDs and Cisco Security Advisory for more information | **High** | * Upgrade to the relevant fixed version referenced in Cisco bug ID CSCvp64857 |
|  | 10.11.30.1 | Cisco Application Policy Infrastructure Controller Privilege Escalation (cisco-sa-20190501-apic-priv-escalation)  - According to its self-reported version, Cisco Application Policy Infrastructure Controller (APIC) is affected by a vulnerability in the FUSE filesystem functionality. This is due to insufficient input validation of CLI commands. An authenticated, local attacker can exploit this by alter certain definitions in a affected file, allowing them to execute commands and gain root privilages.   Please see the included Cisco BIDs and Cisco Security Advisory for more information | **High** | * Upgrade to the relevant fixed version referenced in Cisco bug ID CSCvn09779 |
|  | 10.11.30.1 | Cisco Application Policy Infrastructure Controller Multiple Vulnerabilities (cisco-sa-capic-mdvul-HBsJBuvW)  - According to its self-reported version, Cisco Application Policy Infrastructure Controller (APIC) is affected by multiple vulnerabilities, including the following:    - A command injection vulnerability exists in Cisco APIC due to invalid input validation. An authenticated,  remote attacker can exploit this, by sending specially crafted requests, to execute arbitrary commands.   (CVE-2021-1580)   - An arbitrary file upload vulnerability exists in Cisco APIC due to improper access control. An   unauthenticated, remote attacker can exploit this to upload arbitrary files on the remote host.   (CVE-2021-1581)  Please see the included Cisco BIDs and Cisco Security Advisory for more information. | **High** | * Upgrade to the relevant fixed version referenced in Cisco bug IDs CSCvw57577, CSCvw57581 |
|  | 10.11.12.123 10.11.30.1 10.11.30.15 10.11.30.20 | SSL Certificate Cannot Be Trusted  - The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the  server might not be descended from a known public  certificate authority. This can occur either when the  top of the chain is an unrecognized, self-signed  certificate, or when intermediate certificates are  missing that would connect the top of the certificate  chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate  that is not valid at the time of the scan. This can  occur either when the scan occurs before one of the  certificate's 'notBefore' dates, or after one of the  certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature  that either didn't match the certificate's information  or could not be verified. Bad signatures can be fixed by  getting the certificate with the bad signature to be  re-signed by its issuer. Signatures that could not be  verified are the result of the certificate's issuer  using a signing algorithm that Nessus either does not  support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and  identity of the web server. This could make it easier to carry out  man-in-the-middle attacks against the remote host. | **Medium** | * Purchase or generate a proper SSL certificate for this service. |
|  | 10.11.12.123 10.11.30.1 10.11.30.15 10.11.30.20 | SSL Self-Signed Certificate  - The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. | **Medium** | * Purchase or generate a proper SSL certificate for this service. |
|  | 10.11.12.123 | SSH Weak Algorithms Supported  - Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys. | **Medium** | * Contact the vendor or consult product documentation to remove the weak ciphers. |
|  | 10.11.30.1 | Cisco Application Policy Infrastructure Controller Out Of Band Management IP Tables Bypass (cisco-sa-iptable-bypass-GxW88XjL)  - According to its self-reported version, Cisco Application Policy Infrastructure Controller (APIC) is affected by a vulnerability in the out of band (OOB) management interface IP table rule programming. This is due to the configuration of specific IP table entries for which there is a programming logic error that results in the IP port being permitted. An unauthenticated, remote attacker can exploit this, by sending traffic to the OOB management interface, in order to bypass configured IP table rules to drop specific IP port traffic or bypass configured deny entries for specific IP ports.   Please see the included Cisco BIDs and Cisco Security Advisory for more information | **Medium** | * Upgrade to the relevant fixed version referenced in Cisco bug ID CSCvs10135 |
|  | 10.11.30.1 | Cisco Application Policy Infrastructure Controller Stored XSS (cisco-sa-capic-scss-bFT75YrM)  - According to its self-reported version, Cisco Application Policy Infrastructure Controller is affected by a stored  cross-site scripting (XSS) vulnerability in its Web UI component due to improper validation of user-supplied input  before returning it to users. An authenticated, remote attacker can exploit this, by convincing a user to click a  specially crafted URL, to execute arbitrary script code in a user's browser session.   Please see the included Cisco BIDs and Cisco Security Advisory for more information. | **Medium** | * Upgrade to the relevant fixed version referenced in Cisco bug ID CSCvy64858 |
|  | 10.11.30.5 10.11.30.253 | 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. |
|  | 10.11.12.123 10.11.30.253 | SSH Server CBC Mode Ciphers Enabled  - The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.   Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions. | **Low** | * Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption. |
|  | 10.11.12.123 10.11.30.253 | SSH Weak MAC Algorithms Enabled  - The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.  Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions. | **Low** | * Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms. |
|  | 10.11.12.123 10.11.12.210 10.11.30.253 | SSH Weak Key Exchange Algorithms Enabled  - The remote SSH server is configured to allow key exchange algorithms which are considered weak.  This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:   diffie-hellman-group-exchange-sha1   diffie-hellman-group1-sha1   gss-gex-sha1-\*   gss-group1-sha1-\*   gss-group14-sha1-\*   rsa1024-sha1  Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions. | **Low** | * Contact the vendor or consult product documentation to disable the weak algorithms. |

**ตารางที่ 3** รายละเอียดช่องโหว่พร้อมแนวทางการแก้ไข

## ภาคผนวก รายละเอียดรายการ IP ที่ดำเนินการตรวจสอบช่องโหว่

| * Network Group |
| --- |

| 10.11.12.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 10.11.12.72 | 0 | 0 | 0 | 0 | 0 |
| 2. | 10.11.12.123 | 0 | 1 | 3 | 3 | 7 |
| 3. | 10.11.12.210 | 0 | 0 | 0 | 1 | 1 |
| Summary | | 0 | 1 | 3 | 4 | 8 |

| 10.11.30.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 10.11.30.1 | 2 | 10 | 6 | 0 | 18 |
| 2. | 10.11.30.5 | 0 | 0 | 1 | 0 | 1 |
| 3. | 10.11.30.15 | 0 | 0 | 2 | 0 | 2 |
| 4. | 10.11.30.20 | 0 | 0 | 2 | 0 | 2 |
| 5. | 10.11.30.253 | 0 | 0 | 1 | 3 | 4 |
| Summary | | 2 | 10 | 12 | 3 | 27 |



**ตารางที่ 4** แสดงตารางแสดงผลช่องโหว่ Network Cloud