การอ่านรายงานจุดอ่อน

(Vulnerability Assessment)

วัตถุประสงค์การตรวจสอบจุดอ่อน
(Vulnerability Assessment Objectives)

Identifying (Services, ports, OS, IP, etc.)

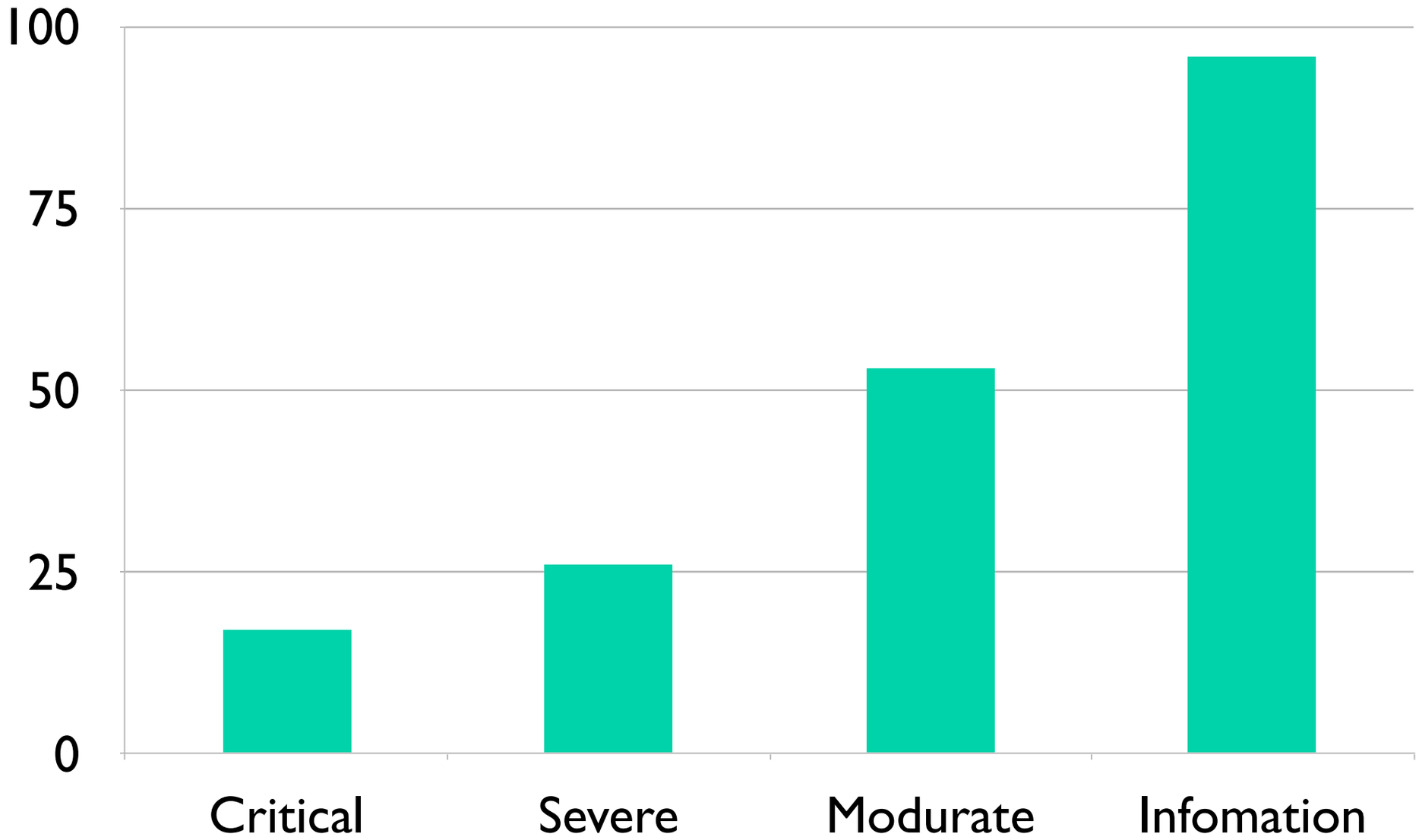
Quantifying

Prioritizing (or ranking)

Identifying

IP Address	Services
203.158.177.3	*DNS*
192.168.12.3	*Application*
172.17.17.1	*Gateway*
172.17.17.245	*Proxy Server*
xxx.xxx.xxx.xx	*Xxxxxxxx*
xxx.xxx.xxx.xx	*Xxxxxxxx*

Quantifying and Ranking



CVSS (Common Vulnerability Scoring System)

เป็นมาตรฐานสำหรับประเมินความรุนแรงของช่องโหว่ของระบบคอมพิวเตอร์ ซึ่งอยู่ภายใต้การดูแลของ *NIST (National Institute of Standards and Technology)* มีตัวชี้วัดเป็นจากการประเมินของผู้เชียวชาญเป็นช่วงคะแนนตั้งแต่ 0-10

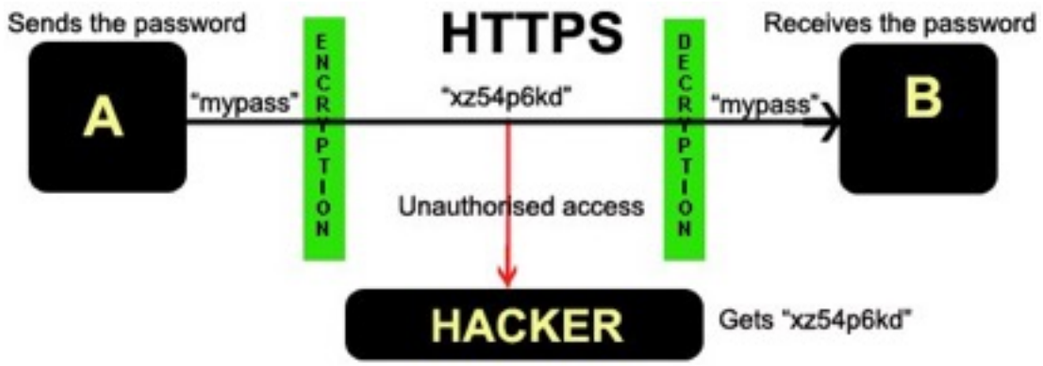
High 7-10	critical 7.5-10
Medium 4-6.9	Severe 5-7.4
LOW 0-3.9	Modurate 3-4.9
	infomation < 2.9

ความเสี่ยงระดับสูง (Critical)

<u>ความเสี่ยงระดับสูง (Critical)</u> มีความเสี่ยงต่อการบุกรุกได้โดยง่าย ผู้บุกรุกสามารถใช้ช่องโหว่ที่ตรวจพบนี้โจมตีระบบและสามารถควบคุมระบบได้ทั้งหมด (Full Control) ควรจะต้องแก้ไขโดยเร่งด่วน **(CVSS Score 7.5-10)**

ความเสี่ยงระดับปานกลาง (Severe)

<u>ความเสี่ยงระดับปานกลาง (Severe)</u> เป็นความเสี่ยงที่ผู้บุกรุกต้องใช้เวลามากขึ้นในการเจาะระบบ ไม่อาจเข้าถึงได้ทันทีแต่อาจเป็นองค์ประกอบที่ช่วยในการโจมตีสำเร็จ **(CVSS Score 5-7.4)**

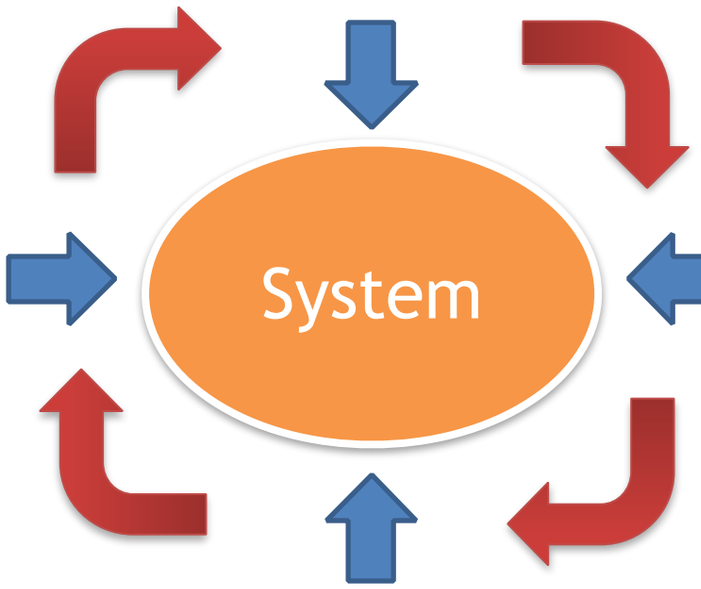


ความเสี่ยงระดับต่ำ (Modulate)

<u>ความเสี่ยงระดับต่ำ (Modulate)</u> เป็นช่องโหว่ที่ผู้บุกรุกไม่สามารถเจาะเข้าสู่ระบบได้โดยใช้ประโยชน์จากช่องโหว่ระดับปานกลางอย่างไรก็ตามเพื่อความสมบูรณ์แบบของการสร้างความมั่นคงปลอดภัยให้แก่ระบบเพราะช่องโหว่ดังกล่าวอาจพัฒนาเป็นช่องโหว่ที่มีความรุนแรงได้ในอนาคต **(CVSS Score 3.0 - 4.9)**

การตรวจสอบช่องโหว่ (System)

Operating System
Microsoft Windows
Solaris
Ubuntu Linux
OSX ,IOS , Android



IP Address
172.17.12.1
203.158.144.2
61.19.12.2
xxx.xxx.xxx.xxx

Program, Version, and Configuration

IIS , Apache , PHP,ASP

Ports
21,22,53,80,88,123,161,1433,3389

การตรวจสอบช่องโหว่ (WEB Site)

.net framework

PHP

ASP

JAVA

การตรวจสอบช่องโหว่

OWASP Top 10 - 2013 (New)

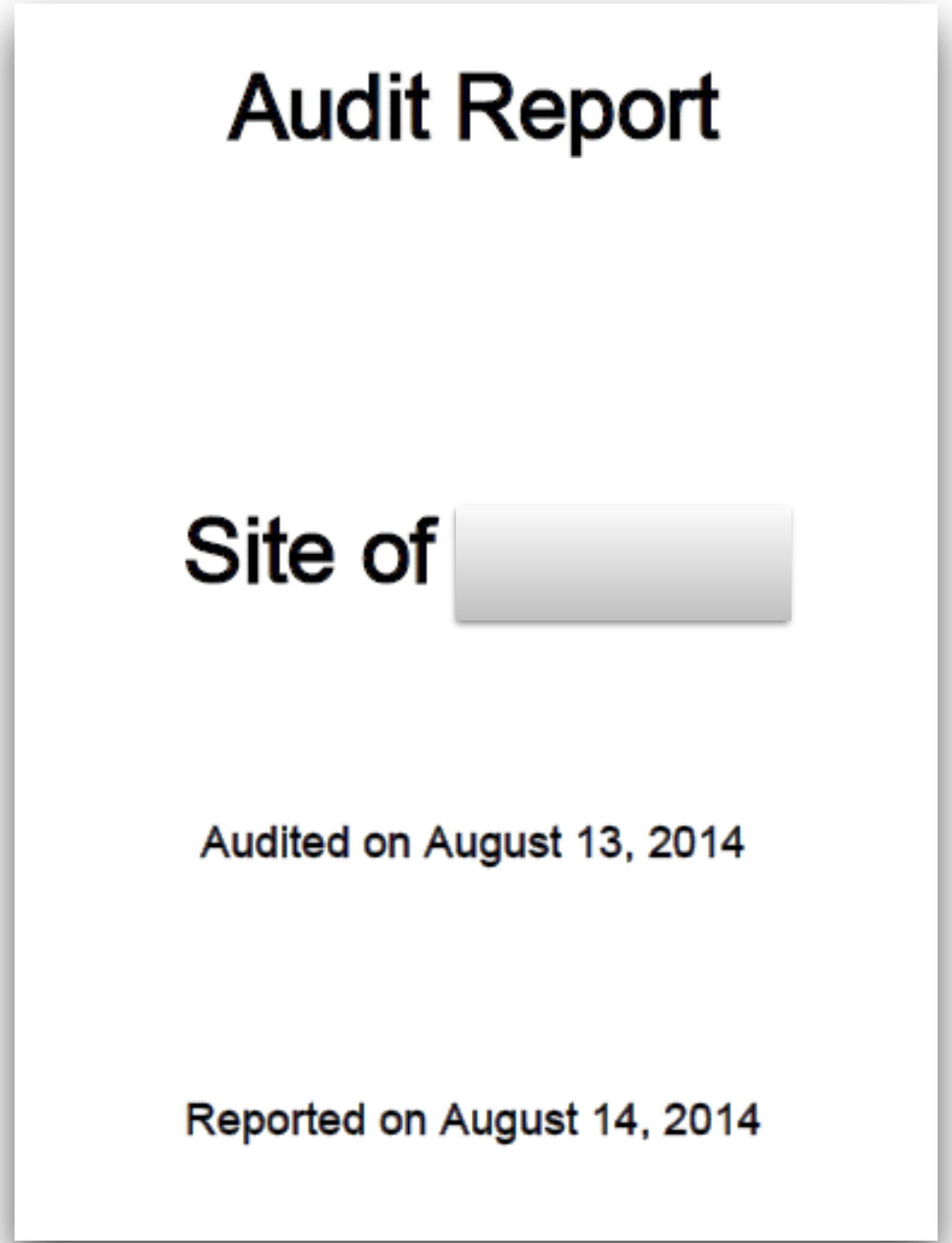
A1 - Injection
A2 - Broken Authentication and Session Management
A3 - Cross-Site Scripting (XSS)
A4 - Insecure Direct Object References
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Missing Function Level Access Control
A8 - Cross-Site Request Forgery (CSRF)
A9 - Using Known Vulnerable Components
A10 - Unvalidated Redirects and Forwards

https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013
https://www.facebook.com/groups/owaspthailand/

Report (Components)

1. Cover
2. Executive Summary
3. Discovered System
4. Discovered and Potential Vulnerabilities
    1. Vulnerability details
    2. Solutions *****

Email Report



Email Report

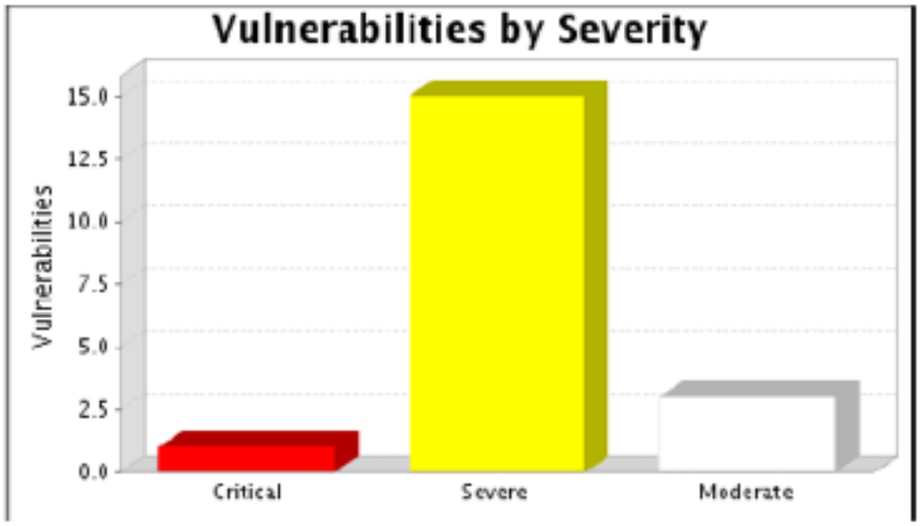
1. Executive Summary

This report represents a security audit performed by Nexpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
Synerry	August 13, 2014 03:14, GMT	August 14, 2014 13:44, GMT	1 days 10 hours 29 minutes	Success

There is [redacted]nough historical data to display overall asset trend.

The audit was performed on one system which was found to be active and was scanned.



There were 19 vulnerabilities found during this scan. One critical vulnerability was found. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 15 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 3 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.

Audit Report

2. Discovered Systems

Node	Operating System	Risk	Aliases
172.17.17.119	Microsoft Windows Server 2008 R2, Standard Edition SP1	4,773	•WIN-AC75QSO1CLR

3. Discovered and Potential Vulnerabilities

The information in this section is based on filtered vulnerability data. View the filters in the following table.

Filter	Setting
Vulnerability severity levels included	Critical and severe

3.1. Critical Vulnerabilities

3.1.1. PHP Vulnerability: CVE-2014-3515 (php-cve-2014-3515)

Description:

The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.

Affected Nodes:

Affected Nodes:	Additional Information:
172.17.17.119:80	Running HTTP serviceProduct IIS found in fingerprint is not HTTPDProduct IIS exists -- Microsoft IIS 7.5Vulnerable version of component PHP found -- PHP 5.4.24

Email Report

Vulnerability Solution:

- Upgrade to PHP version 5.4.30

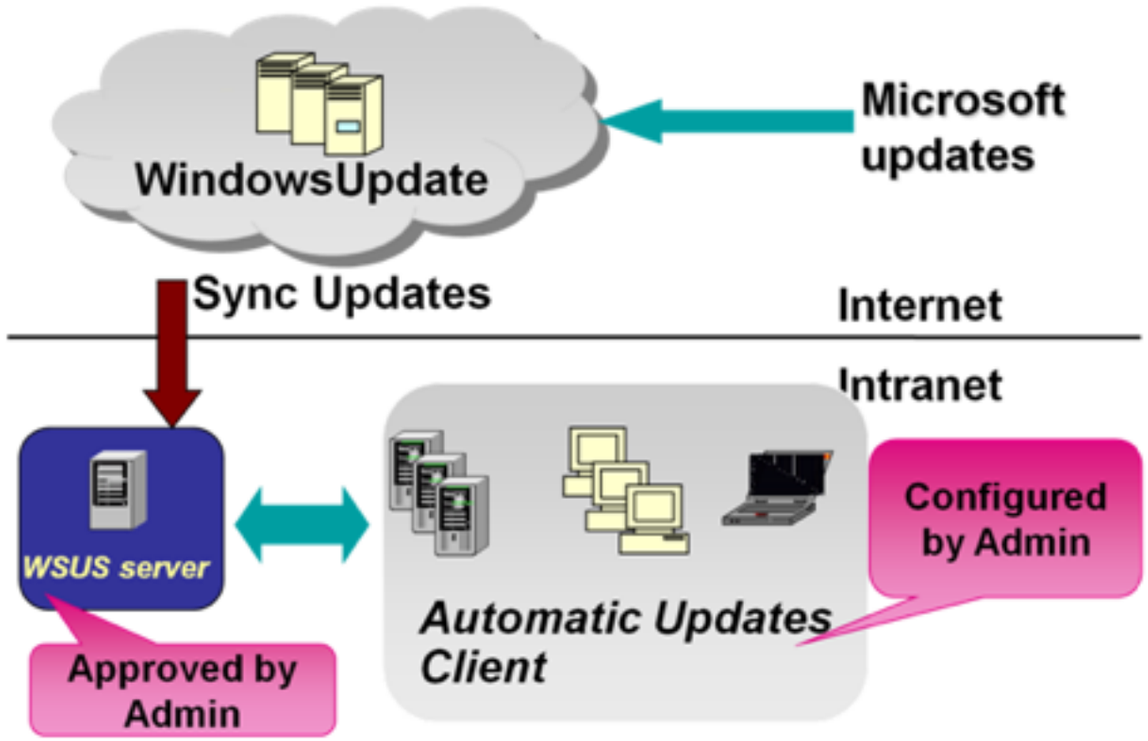
  Download and apply the upgrade from: http://www.php.net/releases/

- Upgrade to PHP version 5.5.14

  Download and apply the upgrade from: http://www.php.net/releases/

ปิดช่องโหว่ Hardening

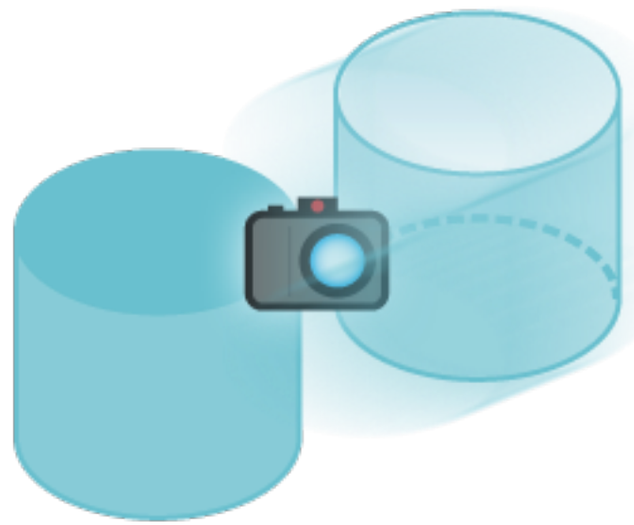
- Update Services Pack and Patch
- Upgrade Programs
- Update Configure
- Disable Unused Services



แนวทางการป้องกันก่อนดำเนินการ Patch

Backup Services

Time:18.00



การดำเนินการตรวจสอบระบบ Cloud

Schedule Scan

Vulnerability Scan	Report
1-15	16-31

1-31 ของทุกเดือน

แนวทางการแจ้งเตือน

ค้นพบจุดอ่อนครั้งที่ 1

ผู้ดูแลระบบ
ผู้บริหาร

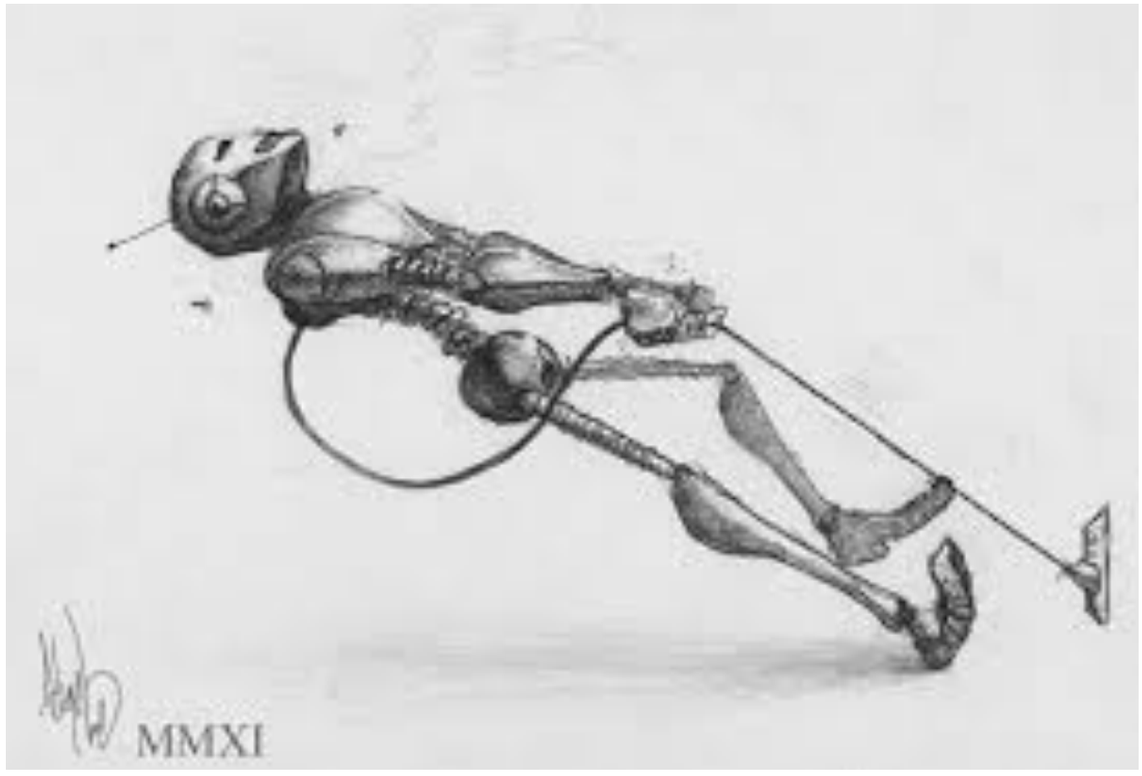
แนวทางการแจ้งเตือน

ค้นพบจุดอ่อนครั้งที่ 2

ผู้ดูแลระบบ
ผู้บริหาร

แนวทางการแจ้งเตือน

ค้นพบจุดอ่อนครั้งที่ 3



คำถาม ?

พงศ์ระพี นาคมณี

วิศวกรความมั่นคงปลอดภัยสารสนเทศ

pongrapee.narkmanee@ega.or.th

02-6126000(4303)