CYBERSEC 2025 臺灣資安大會 | 4/15-4/17 臺北南港展覽二館

SECOPS FORUM

SECOPS FORUM

漏洞補不完！但更付不起企業失控的風險！一起來探討如何掌握漏洞管理的關鍵吧！

TEAM CYBERSECURITY

Resen Tuan

趨勢科技 / Information Technology

Sr. Engineer

Who am I?

- **Resen Tuan**
- **Trend Micro - AMEA IT**
  - Endpoint Security / Event / Product support
- **Certificate**
  - CCNA / RHCE / CEH / ECSA / CHFI / CompTIA security+

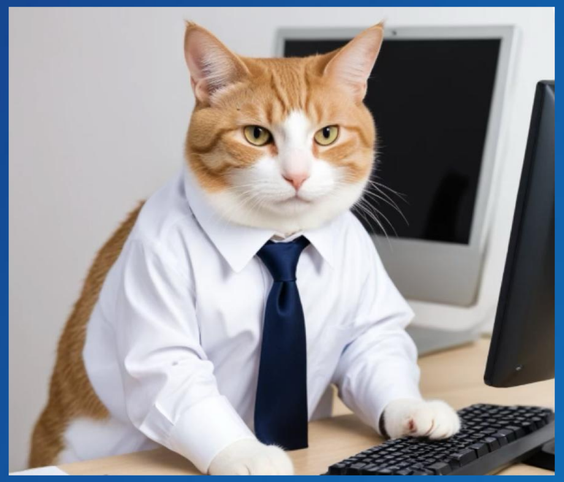
漏洞管理實務與日常維運：資產盤點與弱點管理的實踐

Agenda：

- 為何要落實 Vulnerability Management
- Patch 的 PDCA
- 趨勢科技的實際做法
- 進階 & 自動化 & 工具運用

剛踏入IT領域的新鮮人

曾經你以為你是...



#修電腦？

亂入梗圖

金錢借貸請自行衡量

但事實上 你更像是

有耐心的傳道士 引領著user ~ 慢 ~ 慢 ~ 變 ~ 好！

雖然
生活總是不按牌理出牌
但我想
一切都會慢慢變好

今天不是來傳教，學科學的人，需要有科學的精神與態度，但...有些事無法用科學來解釋！

東方神秘的力量

科學的盡頭 玄學？

圖片來源：https://www.league-funny.com/gossiping/article-350105

我們不迷信

但往往很多時候...

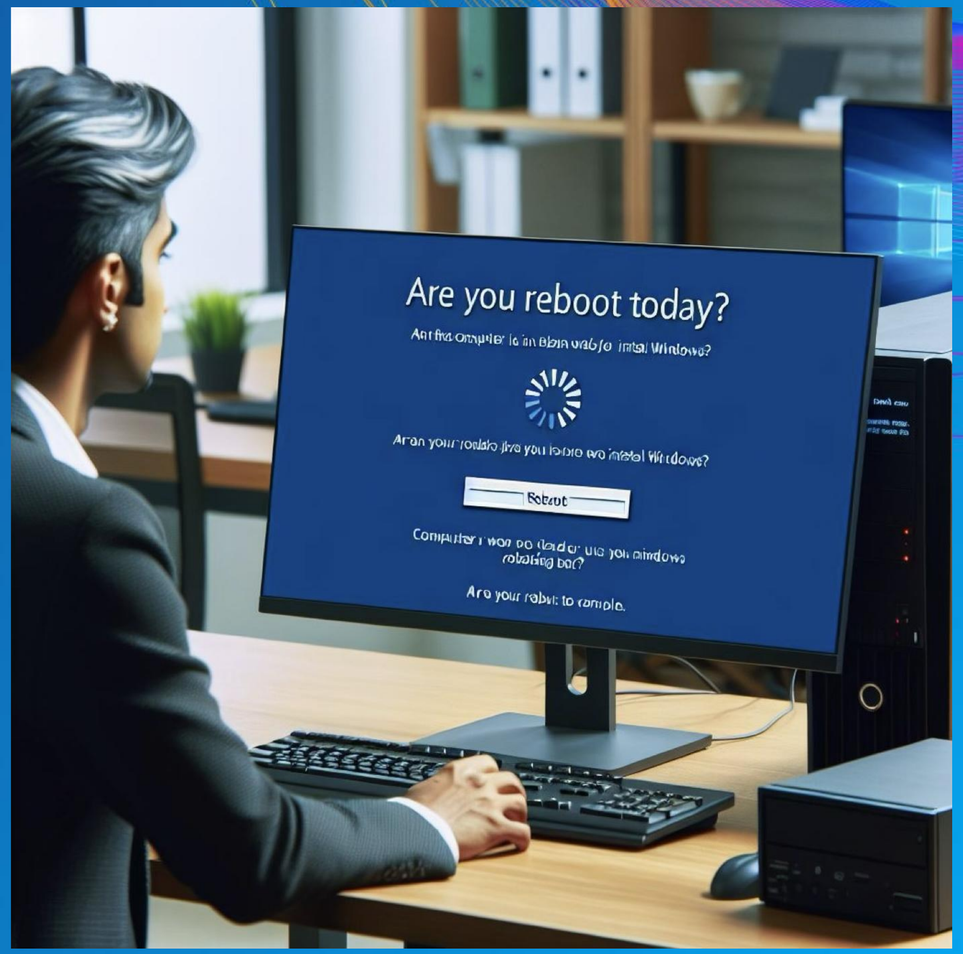
標題 [問卦] 為什麼公司的IT一來第一句話就是
時間 Tue Jul 25 17:10:15 2023

“你有沒有先重開過看會不會恢復正常了“

欸 不是吧 真的重開治百病喔？

阿我重開之後用一陣子還是會有問題跑出來啊

現在是只要會重開機就能當ITman了？



更不用說這種

IT 神秘力量

乖乖 VS 靠得住

拿出你的耐心

要開始了!

資安大哉問：弱點管理到底如何落實?

公司為 ISO 符規及供應商稽核會付費請廠商定期來弱掃，IT 也定期修補弱點

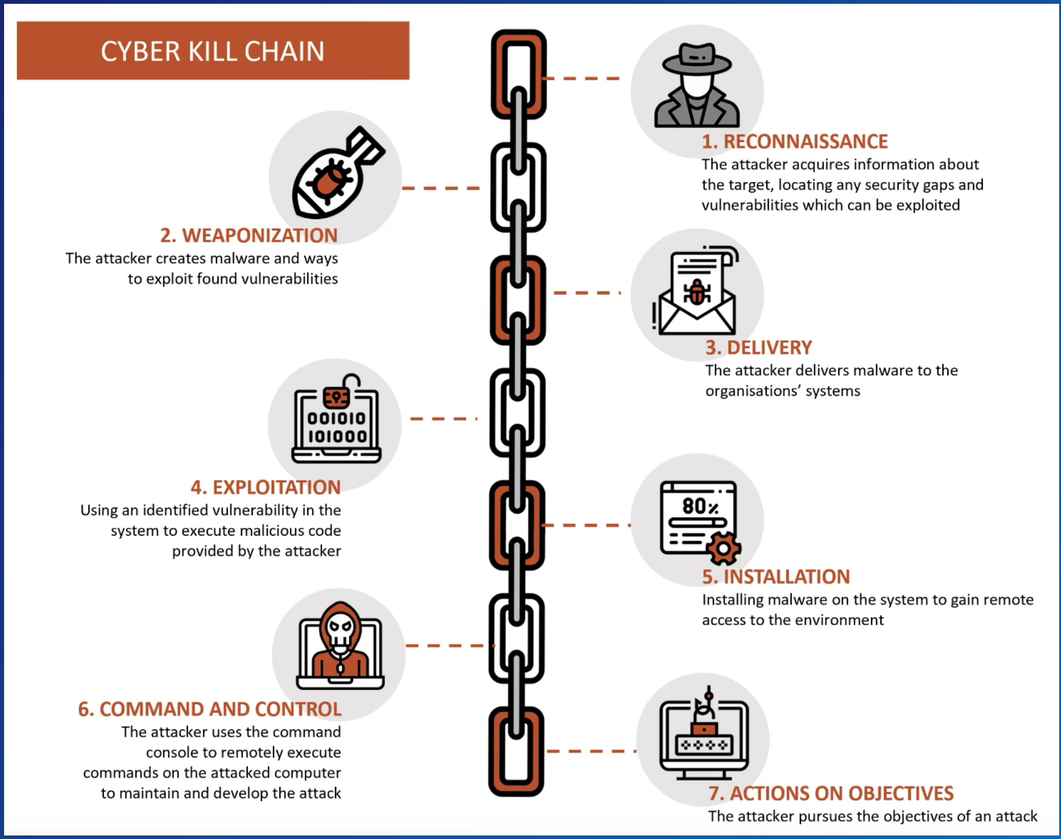
IT 主管

弱點時常新增變化，種類多又雜要在時間內完成全部修補是不可能的。會優先處理被告知的重大弱點，其它就儘量了

IT 維運

駭客 在忙些什麼

他們比你想的做了更多...



Lockheed Martin 公司所開發的「Cyber Kill Chain」(網路攻擊程序) 框架：

- 偵查：蒐集有關攻擊目標以及攻擊手法的相關情報。
- 武器化：開發可攻擊資安漏洞的惡意程式。
- 派送：經由網路釣魚郵件或其他管道派送惡意程式。
- 攻擊漏洞：將惡意程式送入企業系統內部。
- 安裝：安裝後門程式或遠端存取木馬程式讓駭客能隨意進出。
- 幕後操縱 (C&C)：取得企業系統與網路的控制權。
- 達成行動目標：蒐集、加密、擷取企業內的機密資訊。

圖片參考來源：https://seqred.pl/en/cyber-kill-chain-what-is-it-and-how-to-use-it-to-stop-advanced-methods-of-attack/

https://www.trendmicro.com/zh_tw/research/24/d/red-team-exercises-examples.html

駭客做了這麼多功課 那IT呢?

是不是也需要些什麼程序來檢查 - PDCA

計劃 (Plan)

識別漏洞：評估安全漏洞，確定需修補的範圍。
制定策略：制定管理策略，優先級、時間表和資源分配。
風險評估：評估風險影響，確保不造成負面影響。
資源分配：確定資源，確保過程順利進行。

執行 (Do)

部署更新：按照計劃部署，確保都得到更新。
測試更新：先在測試環境進行，再到生產環境，確保有效性和穩定性。
教育訓練：對相關員工進行培訓，確保他們了解更新過程和可能的影響。

檢查 (Check)

監控系統：監控狀況，確保更新已成功應用且沒有引發新的問題。
審核過程：定期審核更新管理過程，確保符合既定的策略和標準。
收集反饋：從用戶和技術團隊收集反饋，了解效果和潛在問題。

行動 (Act)

改進措施：根據檢查階段的結果，採取必要的改進措施，改善更新管理過程。
更新文檔：更新相關文檔和流程，確保未來的更新管理更加高效。
持續改進：根據最新的安全威脅和技術，不斷改進更新管理策略和方法。

#大公司？
#小公司？

事前準備

今天盤點了嗎?

- **為什麼要做資產盤點?**
  - IT 資產盤點的目的? 確保所有資產的完整性與可視性
    - 身為IT 至少要知道自己家網路中有些什麼東西
  - IT 資產分類：~~硬體、軟體、網路設備、數據等~~
    - 凡會 “連上網路” 的設備請都抓進來! 重要主機分級! Owner是誰要知道!
  - 資產盤點常用工具：ex CMDB / Intune / MDM / IPAM / Excel …etc
    - 看看手上有哪些武器，即使Excel 也很好用...

#連上網路
#誰的機器

趨勢為例 資安政策

制定適合組織的管理政策

更新管理政策		
週期 弱點更新	有 加入AD Domain	WSUS / GPO
	沒 加入AD Domain	(重要主機) by 3rd party Tools agent
緊急 弱點更新	72小時內手動更新	
無法更新	集中Firewall單獨網段 ACL控制	

稽核管理政策		
定期弱掃	對外服務	每天 by 3rd party tool 定期去scan
	作業系統+應用程式	By Agent 定期檢查
未修補清單	每週產生超過90天內修補清單建案追綜並通知主管	

IT 管理計畫

Patch 範例

漏洞管理策略：

- 漏洞管理：依”服務“重要性區分
- 漏洞管理周期：多久掃一次？掃到後多久內要修？如何驗證修復？再掃到如何處置？

定期掃描：

- 掃描頻率：如何確定掃描的頻率？
- 自動化工具：依服務選定適合的工具
- 掃描範圍設定：確保全面覆蓋，避免盲點

修復與更新管理：OS vs Service

- 修復計畫：修復優先權 (依CVSS分數)
- 更新管理流程：更新的測試與部署流程
- 修復記錄與驗證：確保修復有效性

持續改進：

- 報告與分析：定期生成報告並分析
- 團隊培訓：強化團隊的安全意識與技能
- 持續改進策略：新的安全措施或方法

依自己公司的制定最適合的做法，盡可能的patch，降低風險。

趨勢為例 檢查些什麼

制定最低要求基準點

• AV Product Installation Scan	• 確保每個client 都有裝防毒
• Firewall Rule Scan	• 確認防火牆設定(驗證ACL)
• MS Patch Compliance Scan	• 微軟的更新檢查確認
• Not Joined to Domain Scan	• Join domain的檢查
• Readable/Writable Share Scan	• File share 檢查 (allow everyone)
• Weak Password Scan	• P@ssw0rd;12345678;qwerty123
• System Vulnerability Scan	• 弱掃 / OS ; Service ; Application

不需要的服務不要開，逐步趕羊的方式限縮調整。

有政策和項目了，怎麼掃

尋找工具及方法

- 定期掃描：
  - 掃描頻率：掃描的頻率？ 掃些什麼？ 最低要求門檻？為何這麼做?
  - 可以用的**武器**工具：ex Nessus / rapid7 / Qualys / OpenVAS / NMAP / CREM
  - 掃描範圍設定：凡會 “連上網路” 的設備請都抓進來 (確保全面覆蓋，避免盲點)
  - 掃描的目標：服務重要性的優先權

#好用的工具值得投資

CREM; Cyber Risk Exposure Management

掃到後，怎麼修?

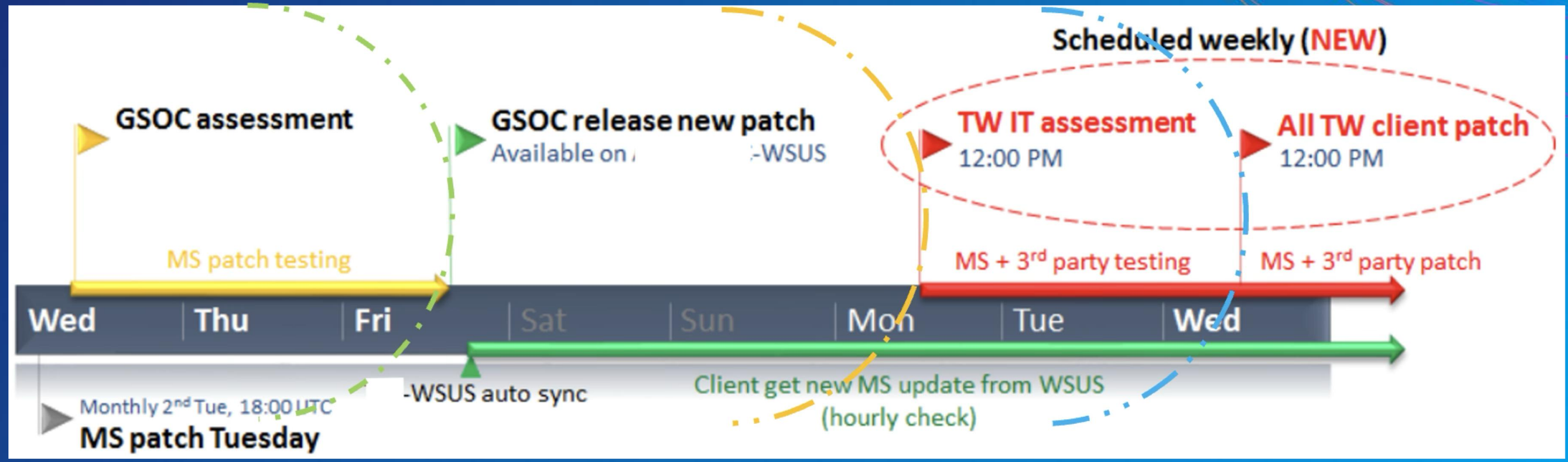
分時 / 分批 / 分次

- 修復與更新管理:
  - 修復計畫：設定修復優先級（依據CVSS分數）or 主機重要性
  - 更新管理流程：更新的測試與部署流程
  - 修復記錄與驗證：確保修復有效性的步驟

#照單全收?
#因地制宜!?

趨勢為例 週期性弱點更新流程

Review更新清單 → WSUS更新列表 → 分群更新 → 定期弱掃（OS+AP） → 未修補電腦稽核

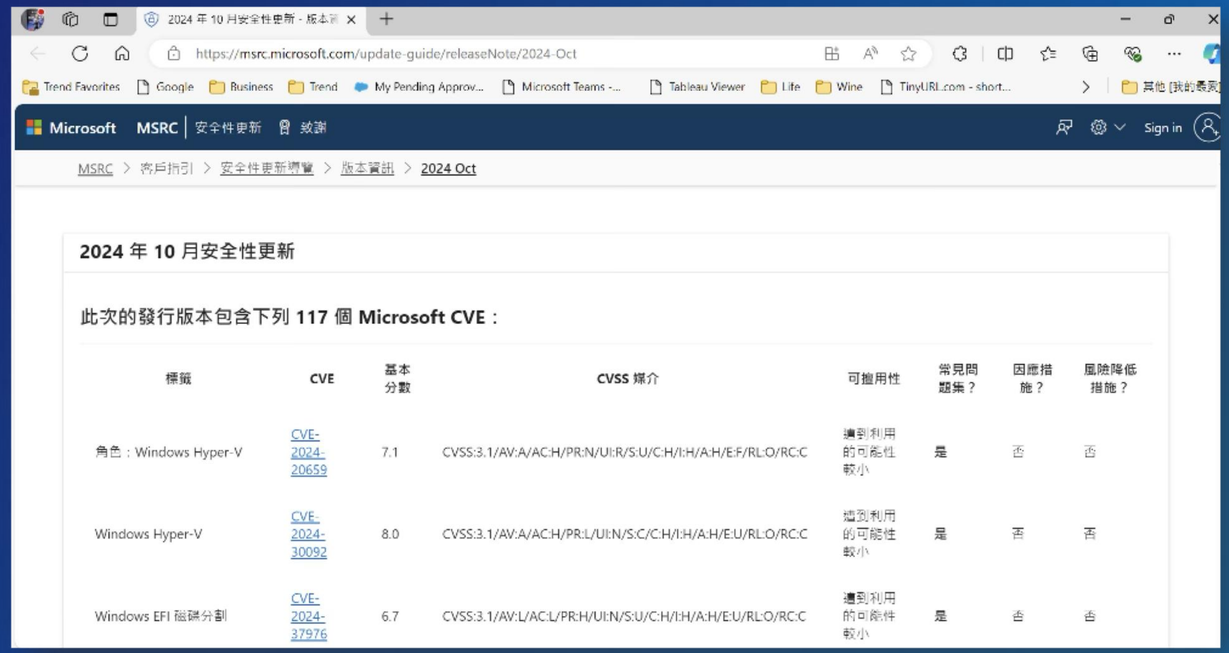


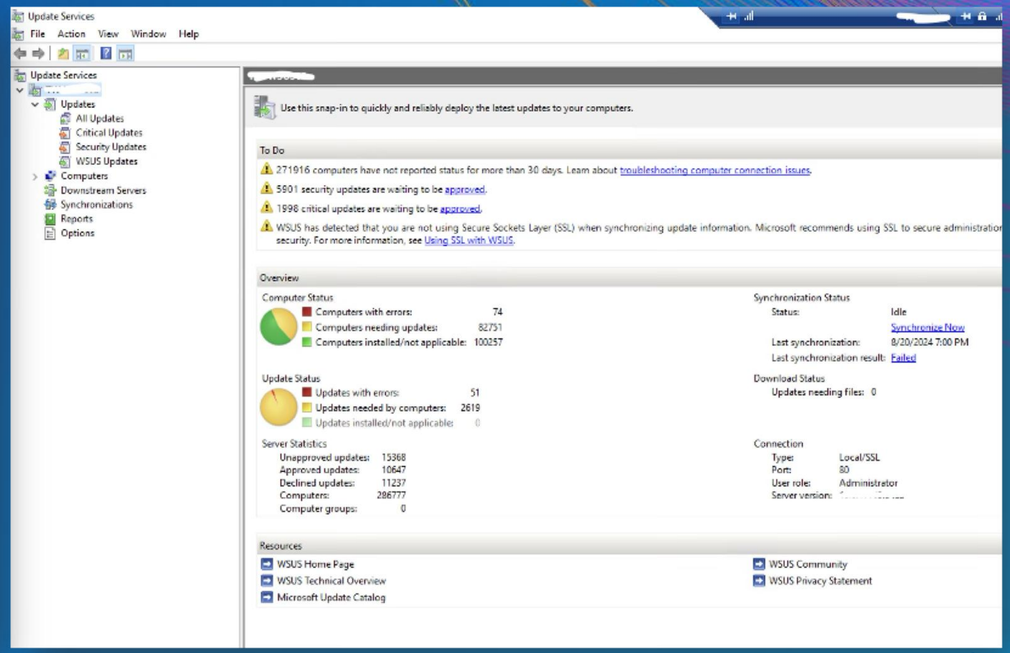
裝完請務必 重開！ * 很重要！

#patch裝完更要重開機！

趨勢為例 實作設定參考

- 查看企業現行OS版本清單其遭利用的可能性+ 3天觀察期(網路資訊)
- 有疑慮的CVE在WSUS取消更新該KB(機率低)



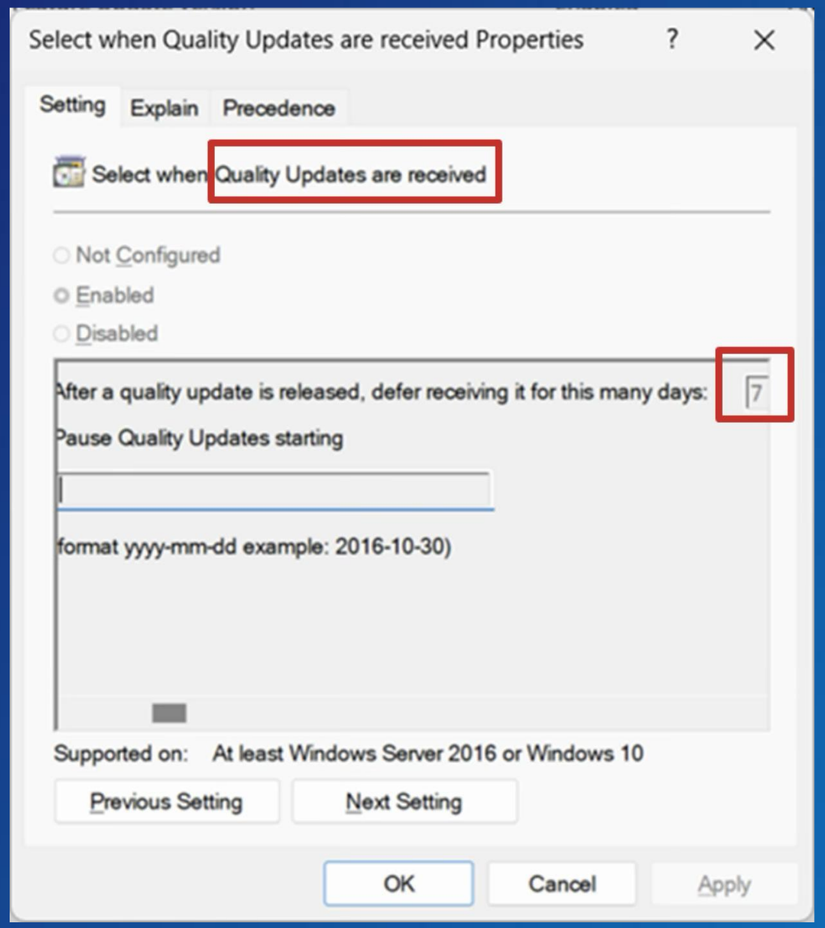


#WSUS retired
#WUfB

https://msrc.microsoft.com/update-guide/vulnerability

https://learn.microsoft.com/en-us/windows/release-health/windows-message-center#3482

趨勢為例 GPO 設定 – 每月 Patch 更新



Update ring settings Edit

Update settings	
Microsoft product updates	Allow
Windows drivers	Block
Quality update deferral period (days)	7
Feature update deferral period (days)	180
Upgrade Windows 10 devices to Latest Windows 11 release	No
Set feature update uninstall period (2 - 60 days)	30
Servicing channel	General Availability channel
User experience settings	
Automatic update behavior	Reset to default
Option to pause Windows updates	Enable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	7
Deadline for quality updates	3
Grace period	2
Auto reboot before deadline	Yes

#Win10 EOL
#WUfB

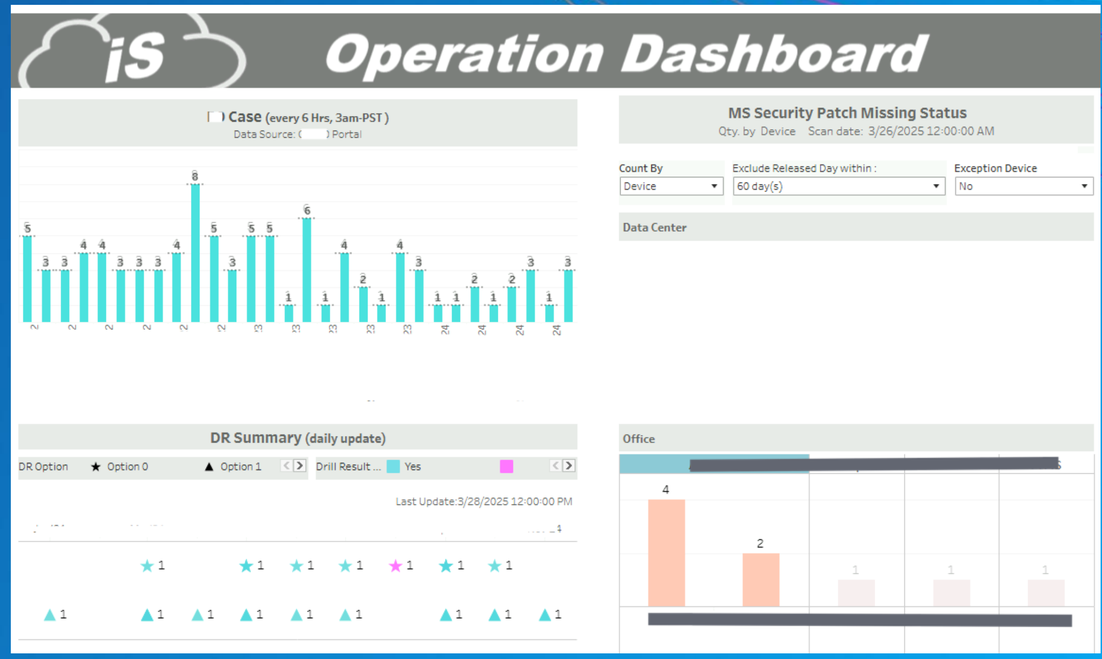
別忘了前面提到的 分時 / 分次 / 分批！很重要！！

修完修完後 然後呢?

IT每個月的成果別忘了

#季報
#年報

- 持續改進:
  - 報告與分析: 定期生成報告並分析漏洞趨勢
  - 團隊培訓: 強化團隊的安全意識與技能
  - 持續改進策略: 實施新的安全措施和技術升級
  - 相關規範: 法規及相關認證



#曲線圖

趨勢為例 更新計劃的調整

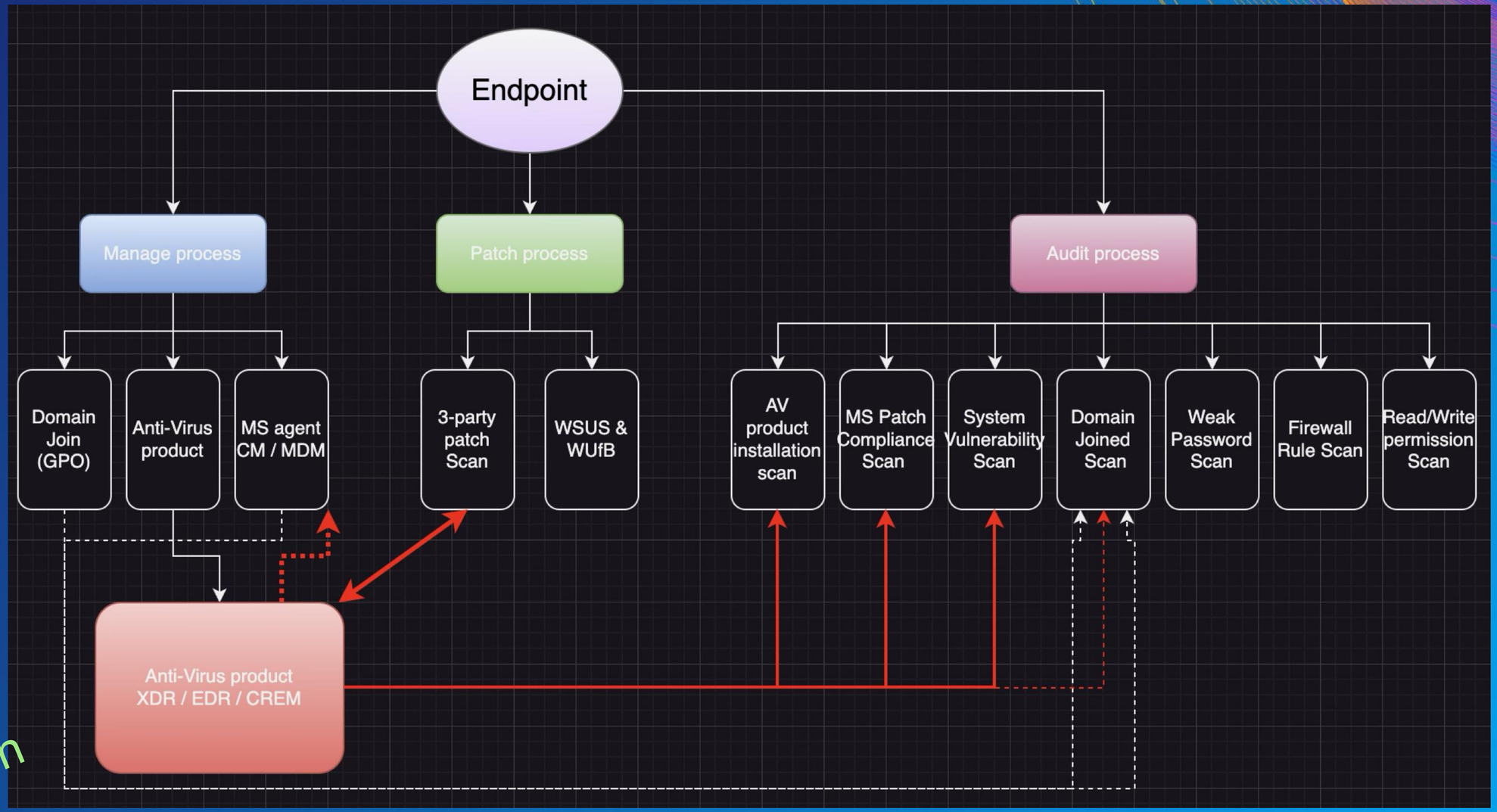
這之前不是看過了?

更新管理政策			
週期 弱點更新	On-premise 環境	•WSUS / GPO •3rd party Tools agent	•Server & Client •Non domain
	SaaS 環境	•MECM / WUfB •WSUS / GPO (WUfB) •3rd party Tools agent	•Client •Server •Non domain
緊急 弱點更新	72小時內手動更新		
無法更新	集中Firewall單獨網段 ACL控制		

#SaaS
#hybrid

另外，除了原有的，是不是還能做些什麼

結合既有的solution 產生其他方式?



#API
#AI
#Coding
#automation

CREM; Cyber Risk Exposure Management

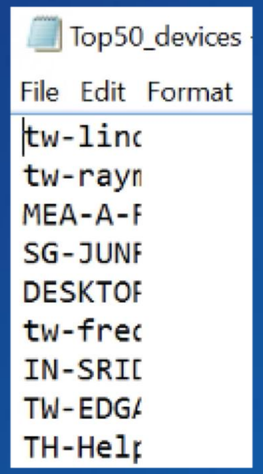
實際例子 - 1

透過XDR API 和增加排程彌補欠缺

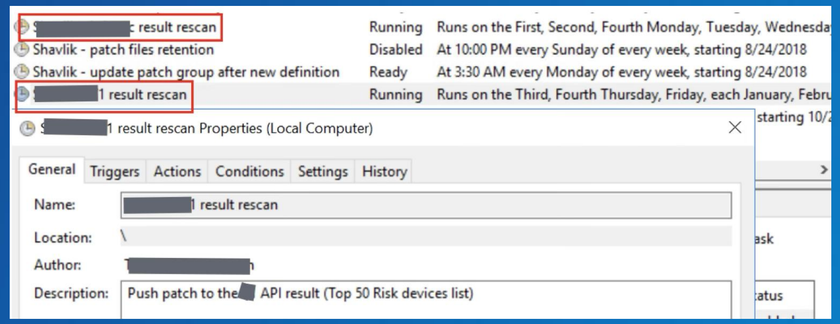
CREM with high CVE device

Device name	Operating system	IP address	Last user	CVE event risk score ↓	Total CVEs
TW-	Windows 11 10.0 (Build 226...	172.31.80.1	An	76	1
LAP	Windows 11 10.0 (Build 226...	10.1.1	ter	76	7
TW-	Windows 11 10.0 (Build 226...	10.1.1	and	76	30
LX-	Windows 10 10.0 (Build 190...	192.1	user	75	41
TW-	Windows 11 10.0 (Build 226...	192.1	ext	75	8
LAP	Windows 11 10.0 (Build 226...	169.25		75	11

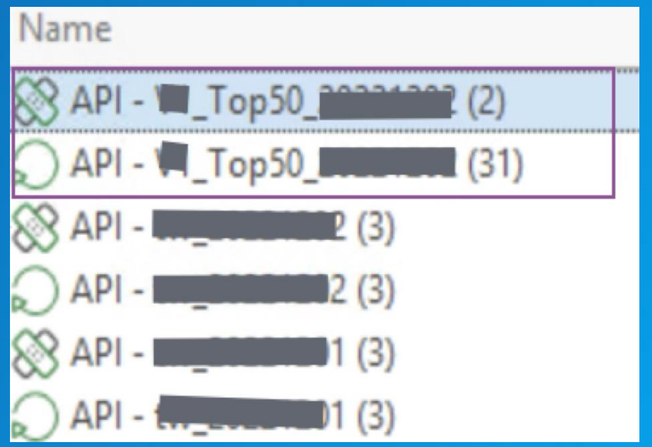
XDR API



Schedule task



3-party patch process



#GPT
#API
#Scan Base

實際例子 - 2

Cisco IOS XE web UI vulnerability - CVE-2023-20198

Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature

Critical

Advisory ID:	cisco-sa-iosxe-webui-privesc-j22SaA4z	CVE-2023-20198
First Published:	2023 October 16 15:00 GMT	CVE-2023-20273
Last Updated:	2023 November 1 15:44 GMT	CWE-420
Version 2.6:	Final	CWE-78
Workarounds:	No workarounds available	
Cisco Bug IDs:	CSCwh87343	
CVSS Score:	Base 10.0	

Download CSAF
Email

Summary

Cisco is providing an update for the ongoing investigation into observed exploitation of the web UI feature in Cisco IOS XE Software. We are updating the list of fixed releases and adding the Software Checker.

Fix information can be found in the Fixed Software section of this advisory.

Our investigation has determined that the actors exploited two previously unknown issues.

The attacker first exploited CVE-2023-20198 to gain initial access and issued a privilege 15 command to create a local user and password combination. This allowed the user to log in with normal user access.

The attacker then exploited another component of the web UI feature, leveraging the new local user to elevate privilege to *root* and write the implant to the file system. Cisco has assigned CVE-2023-20273 to this issue.

- **CVE-2023-20198** has been assigned a CVSS Score of 10.0.
- **CVE-2023-20273** has been assigned a CVSS Score of 7.2.

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

Subscribe

Related to This Advisory

Your Rating:

Average Rating:

5 star 4
4 star 0
3 star 0

Recommendations

Cisco strongly recommends that customers disable the HTTP Server feature on all internet-facing systems or restrict its access to trusted source addresses. To disable the HTTP Server feature, use the **no ip http server** or **no ip http secure-server** command in global configuration mode. If both the HTTP server and HTTPS server are in use, both commands are required to disable the HTTP Server feature.

The following decision tree can be used to help determine how to triage an environment and deploy protections:

- Are you running IOS XE?
  - **No**. The system is not vulnerable. No further action is necessary.
  - **Yes**. Is **ip http server** or **ip http secure-server** configured?
    - **No**. The vulnerabilities are not exploitable. No further action is necessary.
    - **Yes**. Do you run services that require HTTP/HTTPS communication (for example, eWLC)?
      - **No**. Disable the HTTP Server feature.
      - **Yes**. If possible, restrict access to those services to trusted networks.

逐一確認

```
t          >sw01#sh run | i http
no ip http server
no ip http secure-server
t          >sw01#
```

透過script確認

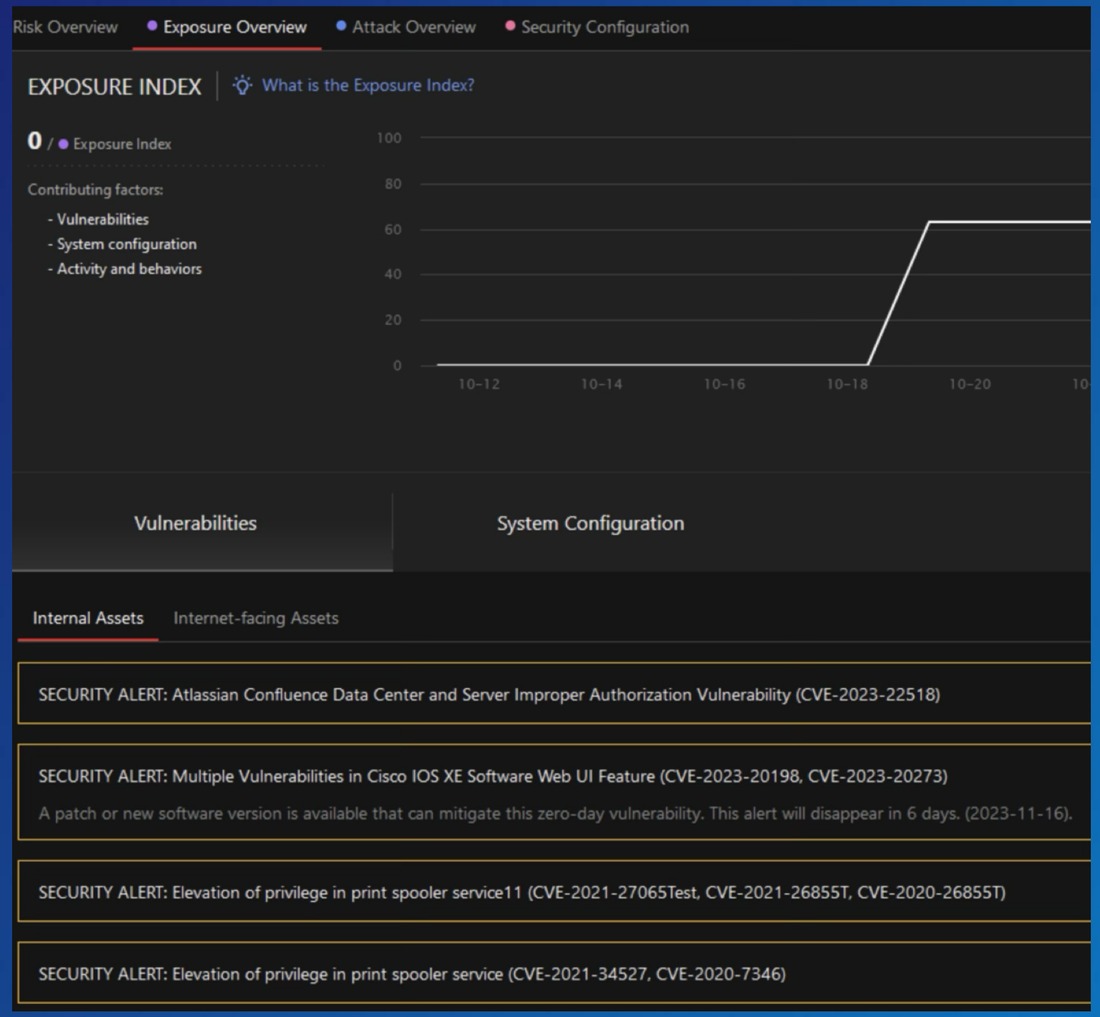
```
D:\Cisco_WebUX test>python iocisco.py 10.1.12.111
[!] Checking http://10.1.12.111:80/%25
    Error: HTTPConnectionPool(host='10.20.6.13', port=8080): Read timed out. (read timeout=10)
[!] Could not determine status of http://10.1.12.111:80/%25
[!] Checking https://10.1.12.111:443/%25
    Error: HTTPSConnectionPool(host='10.1.12.111', port=443): Max retries exceeded with url: /%25 (Caused by ProxyError('
'Cannot connect to proxy.', timeout('timed out')))
[!] Could not determine status of https://10.1.12.111:443/%25

D:\Cisco_WebUX test>python iocisco.py 10.1.111.210
[!] Checking http://10.1.111.210:80/%25
    Error: HTTPConnectionPool(host='10.20.6.13', port=8080): Read timed out. (read timeout=10)
[!] Could not determine status of http://10.1.111.210:80/%25
[!] Checking https://10.1.111.210:443/%25
    Error: HTTPSConnectionPool(host='10.1.111.210', port=443): Max retries exceeded with url: /%25 (Caused by ProxyError('
'Cannot connect to proxy.', timeout('timed out')))
[!] Could not determine status of https://10.1.111.210:443/%25

D:\Cisco_WebUX test>_
```

#nmap

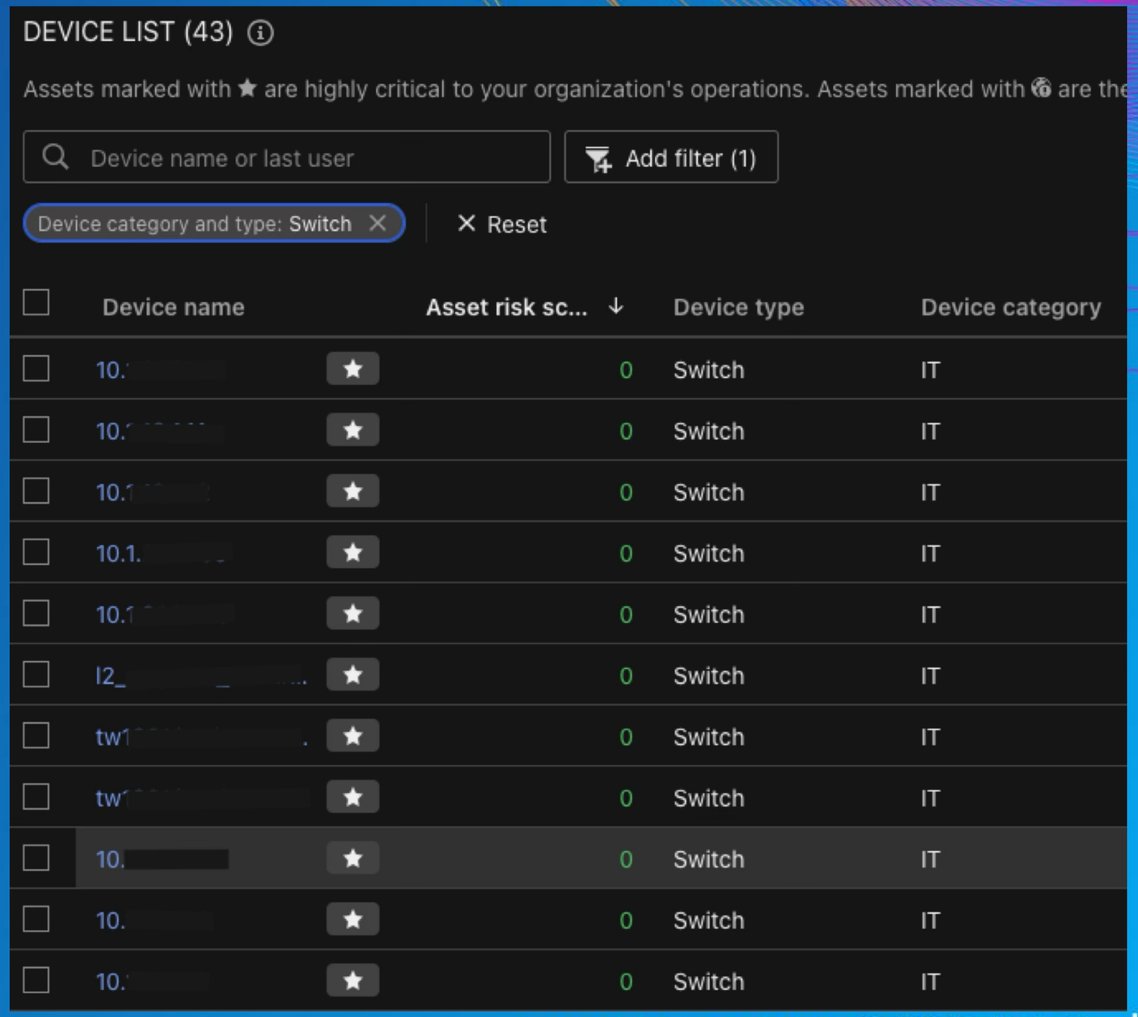
實際例子 – 2 續

如果有其他工具

Exposure Overview - Vulnerability



CREM - devie list



實際例子 – 3

如何快速的盤點? 別忘了你有好朋友GPT

Using PowerShell to Run Nmap
6 messages

With 0 contextual prompts

Hello! How can I assist you today?

Contextual Prompt

if my windows had installed nmap, how to use powershell to run the nmap script to scan a IP range 10.240.40.0/24 this IP range's machine OS version and list how many devices in this IP range

please give me a bash script sample
use the nmap to do the IP
1) ping sweep and list the up IP address and
2) use the result to do the OS scan version and list
3) count the num of result ex win10 = 10 ; win11 = 5 ; win7 = 4

To use PowerShell to run an Nmap script to scan an IP range and determine the operating system versions of the devices within that range, you can follow the steps below. This example will show you how to scan the IP range `[IPAddress]/24` and list the number of devices detected.

1. **Open PowerShell**: First, open PowerShell with administrative privileges.
2. **Run Nmap Command**: Use the `nmap` command to scan the IP range. The `-O` option in Nmap enables OS detection, and the `-oG` option outputs the results in a greppable format, which makes it easier to parse the results in PowerShell.
3. **Parse the Output**: Use PowerShell to parse the output and count the number of devices detected.

Here is a detailed script to accomplish this task:

```
# Define the IP range to scan
$ipRange = "[IPAddress]/24"

# Define the path to the Nmap executable
$nmapPath = "C:\Program Files (x86)\Nmap\nmap.exe"

# Run the Nmap scan with OS detection and output in greppable format
$nmapOutput = & $nmapPath -O -oG - $ipRange

# Initialize a counter for the number of devices
$deviceCount = 0
```

```
Starting Ping Sweep...
Host is up: 10.211.55.1
Host is up: 10.211.55.2
Host is up: 10.211.55.3
Ping Sweep Complete. Found 3 live hosts.
Starting Nmap OS Scan...
Scanning 10.211.55.1...
No OS information found for 10.211.55.1.
Scanning 10.211.55.2...
No OS information found for 10.211.55.2.
Scanning 10.211.55.3...
Nmap Scan Complete.
OS Scan Summary:
OS details: Microsoft Windows 10 1607 - 11 23H2 * 1
Running: Microsoft Windows 10 * 1
Nmap scan report for windows-11.shared (10.211.55.3) * 1
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11 * 1
Script Finished.

PS C:\Program Files (x86)\Nmap>
```

Bash

```
#!/bin/bash

# Target network or IP range
TARGET="192.168.1.0/24" # Replace with your target

# Temporary files
UP_HOSTS_FILE=$(mktemp)
OS_SCAN_FILE=$(mktemp)

# 1. Ping sweep and list up IP addresses
echo "Performing ping sweep..."
nmap -sn $TARGET | grep "Host is up" | awk '{print $5}' > $UP_HOSTS_FILE

if [ ! -s "$UP_HOSTS_FILE" ]; then
  echo "No hosts found up. Exiting."
  rm "$UP_HOSTS_FILE" "$OS_SCAN_FILE"
  exit 1
fi
```

#GPT
#nmap

實際例子 – 3 續

如果有好用的工具

CREM - devie list

DEVICE LIST (22754)

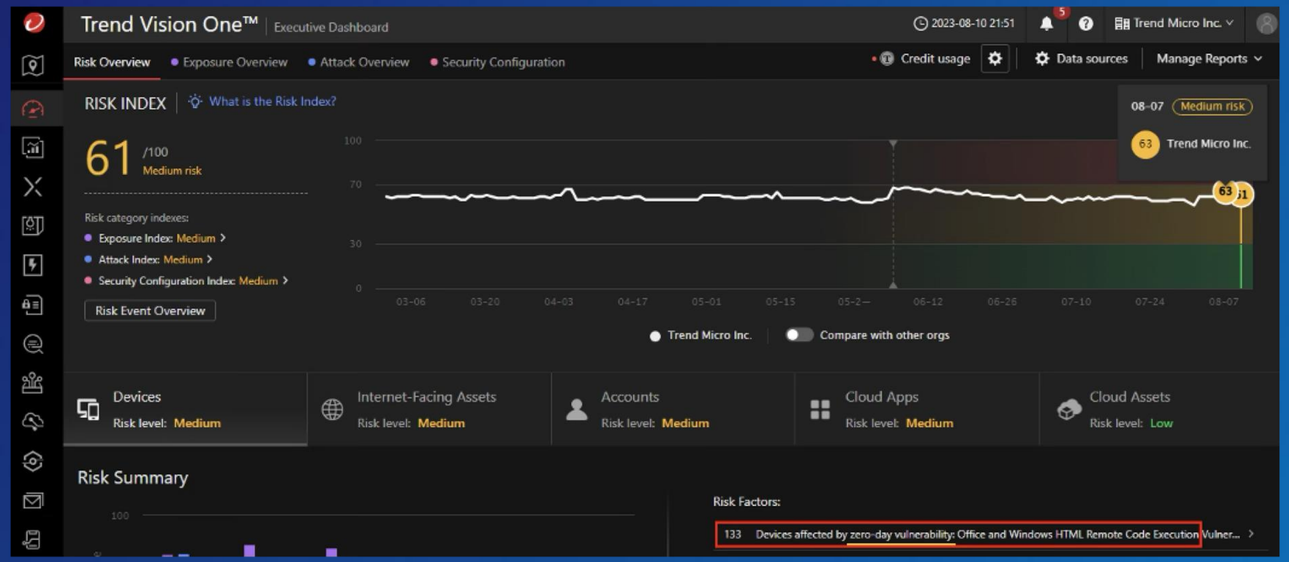
Assets marked with ★ are highly critical to your organization's operations. Assets marked with are the assets that can be connected to from the internet.

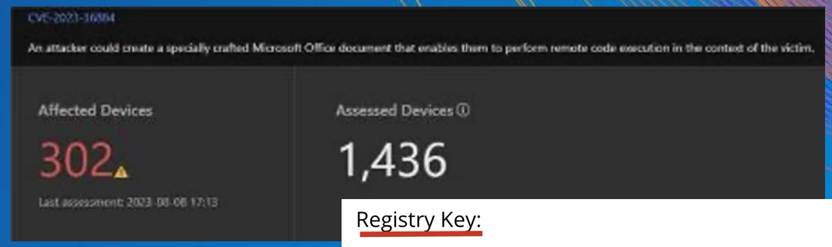
Device name or last user | Add filter

Device name	Asset risk sc... ↓	Device type	Device category	Operating system	IP address
ME	79	Desktop	IT	Windows 11 10.0 (Build 22631)	10.1
TW	79	Desktop	IT	Windows 11 10.0 (Build 22631)	10.2
MY	79	Desktop	IT	Windows 10 10.0 (Build 19044)	192
10.	78	-	-	-	10.
TW	75	Desktop	IT	Windows 11 10.0 (Build 22631)	169
10.	75	-	-	-	10.
10.	75	-	-	-	10.1

實際例子 – 4

Zero day?





A zero-day vulnerability (TMVA1017) published on 2023-08-02 detected

Remediation: Take the available mitigation actions against the vulnerability.

riskLevel:	High
vulnerabilityName:	Office and Windows HTML Remote Code Execution Vulnerability
assetCriticality:	6
publishDate:	2023-08-02T00:00:00
relatedCveId:	CVE-2023-36884
zeroDayId:	TMVA1017
vulnerabilityDescription:	An attacker could create a specially crafted Microsoft Office document that enables them to perform remote code execution in the context of the victim.

Registry Key:
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION

Applications to Add:

- Excel.exe
- Graph.exe
- MSAccess.exe
- MSPub.exe
- Powerpnt.exe
- Visio.exe
- WinProj.exe
- WinWord.exe
- Wordpad.exe

Please ensure that each application name is added as a value of type REG_DWORD with a data value of 1.

AFFECTED DEVICES

Endpoint Sensors have stopped scanning for this zero-day vulnerability because a patch or new software version is available to mitigate this zero-day vulnerability.

Last assessment: 2023-08-21 23:10

#GPO #SCCM #Patch Process #custom script #Virtual Patch

https://www.action1.com/how-to-mitigate-office-and-windows-html-remote-code-execution-vulnerability-cve-2023-36884/

可能需要知道些什麼?

- **Certs NEWS: US cert / HK cert / TW cert / Ithome**
- **Internet resource:**

  www.shodan.io

  www.virustotal.com

  global.sitesafety.trendmicro.com

  owasp.org

- **CyberSecurity NEWS:**

  https://www.trendmicro.com/vinfo/us/security/news

- **Trend Mirco**

  https://asrm.twbu.trendmicro.com/ASRM/3-3-重要主機風險管理實務#使用-workload-protection

總結

- 良好計劃很重要
- 好用的工具很需要
- 平時體質調養也很重要
- 日常環境的水溝蓋清淤
- 呂布治百病！
- 別忘了，你是個有耐心的傳道士！

#吃維他命C就不感冒?
#流感疫苗 不感冒?

Thanks

TEAM CYBERSECURITY