



政府機關資安弱點通報機制 推動規劃

行政院國家資通安全會報技術服務中心

108年11月27日

大綱

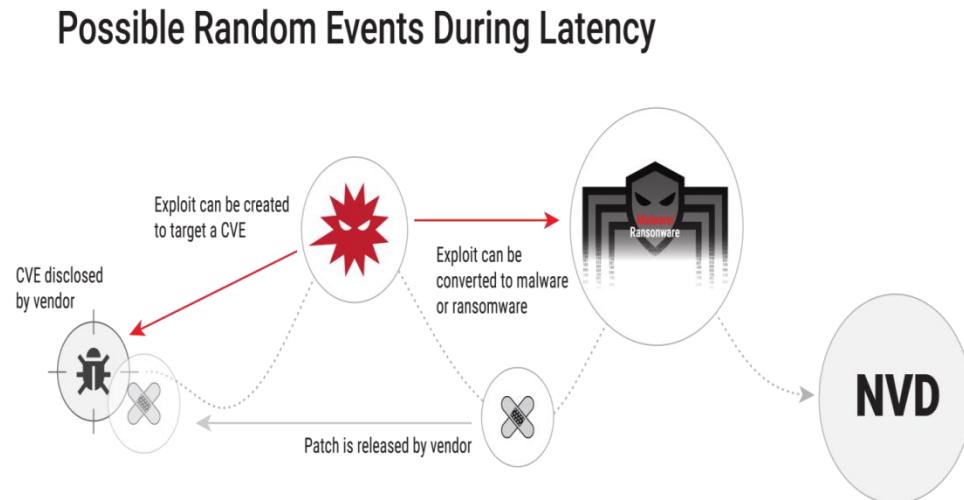
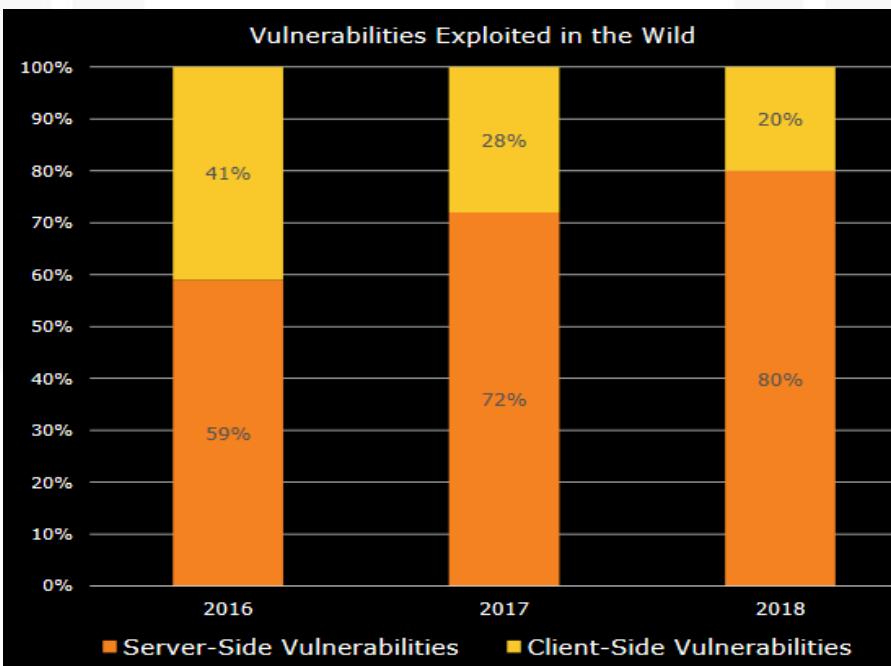
- 前言
- 政府機關資安弱點通報機制
- 系統功能
- 實作建議
- 後續推動重點

大綱

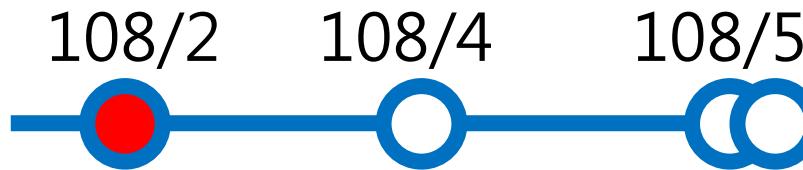
- 前言
- 政府機關資安弱點通報機制
- 系統功能
- 實作建議
- 後續推動重點

資安情勢分析

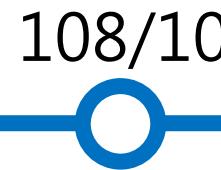
- Skybox Security之資安弱點與威脅報告指出，2018年有80%攻擊，利用弱點影響伺服器端的應用程式，包含對政府機關造成重大影響之Apache struts弱點
- 弱點(CVE)公布後到廠商釋出修補程式之空窗期，是駭客利用的絕佳時機



WinRAR ACE弱點



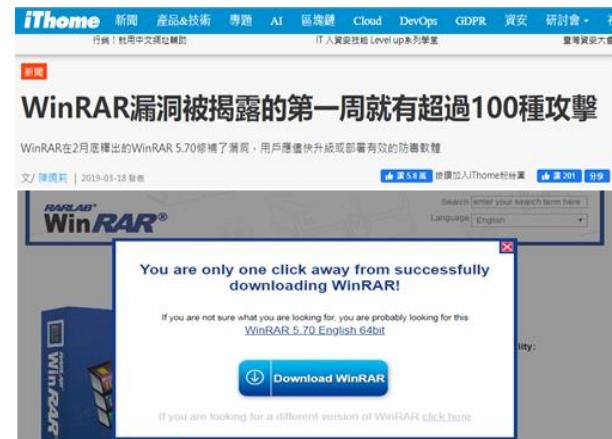
- Check Point於108年2月揭露，WinRAR存在CVE-2018-20250弱點，受影響範圍包含全球5億用戶端
- WinRAR仍使用已於2007年即停止支援之ACE壓縮檔格式，駭客可在ACE壓縮檔中加入惡意程式，當用戶進行解壓縮時會同時將惡意程式放入電腦中，導致電腦每次開機時皆自動執行惡意程式
- 建議儘速升級至WinRAR 5.70以後版本



WinRAR 爆出 10 年未被發現的大漏洞：解壓縮同時會把病毒安裝到電腦裡

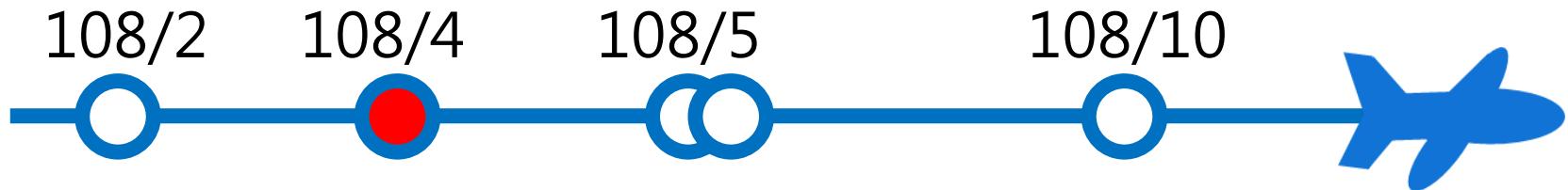
2019/02/23  1,003 分享

unwire.hk

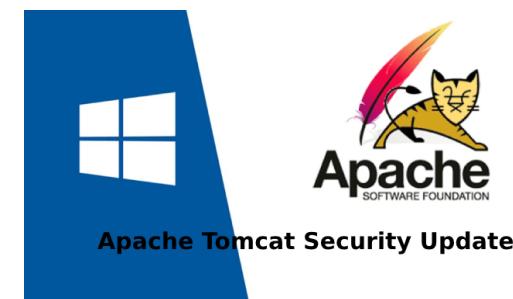


The screenshot shows a news article from iThome. The headline reads "WinRAR漏洞被揭露的第一周就有超過100種攻擊". The article discusses the vulnerability and its impact. At the bottom, there is a download link for WinRAR 5.70 English 64-bit.

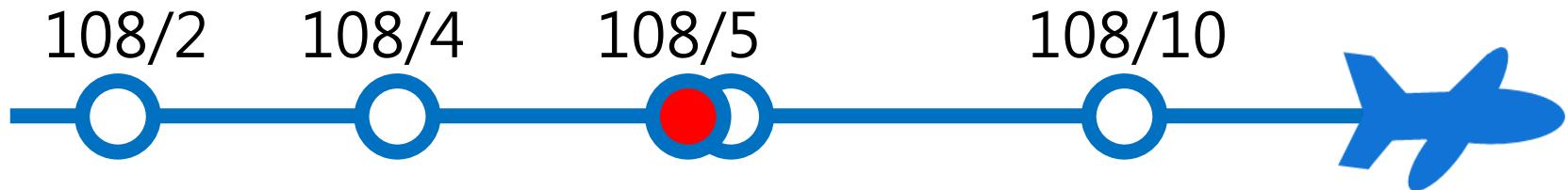
Apache Tomcat弱點



- Apache Tomcat部分版本存在安全性弱點(CVE-2019-0232)，攻擊者可利用此弱點，於目標系統遠端執行程式碼
- Apache Tomcat若安裝於Windows作業系統，且將「enableCmdLineArguments」設為Enable時，以下版本將受此弱點影響
 - 9.0.0.M1至9.0.17以前版本
 - 8.5.0至8.5.39以前版本
 - 7.0.0至7.0.93以前版本



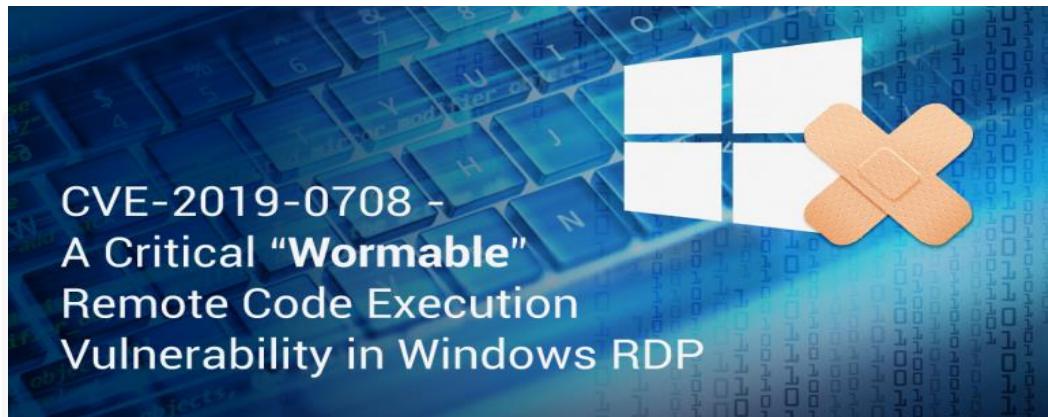
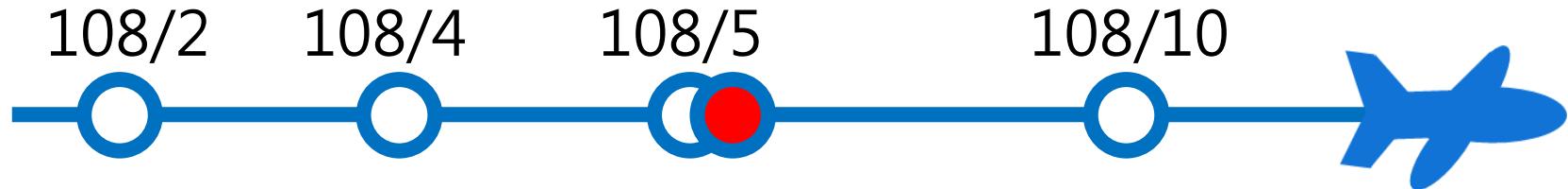
PostgreSQL存在多個弱點



- 108年5月，PostgreSQL釋出更新版，修復多個安全性弱點(CVE-2019-10127~10130)，攻擊者可利用上述弱點執行任意程式碼、繞過安全機制及洩漏資訊
- 受影響版本為PostgreSQL 9.4.22以前版本、9.5.17以前版本、9.6.13以前版本、10.8以前版本及PostgreSQL 11.3以前版本



BlueKeep



iThome 新聞 產品&技術 專題 AI 區塊鏈 Cloud DevOps GDPR 資安 研討會 · 社群 · 商用電腦

新聞

開源安全測試框架Metasploit嵌入BlueKeep攻擊程式

在開源測試框架中嵌入這個針對舊版Windows遠端桌面服務缺陷所打造的攻擊程式，固然可能遭駭客利用，但Metasploit管理方Rapid7認為，此舉對防禦方來說是利大於弊

文/陳曉莉 | 2019-09-09 發表

讚 58 萬 按讚加入iThome粉絲團 讀 97 分享

rapid7 / metasploit-framework

<> Code

Issues 696

Pull requests 60

Projects 2

Wiki

Security

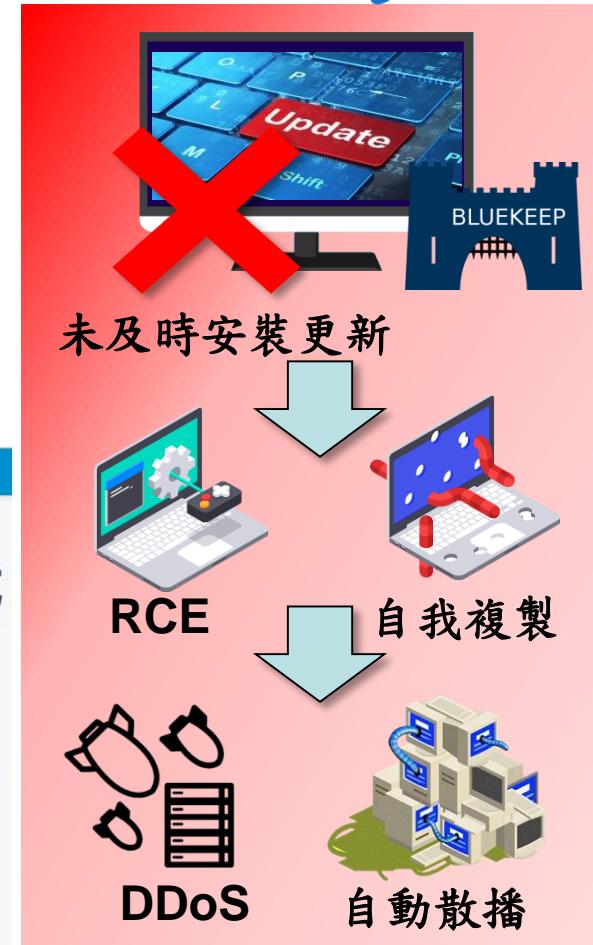
Insights

Watch 1,667

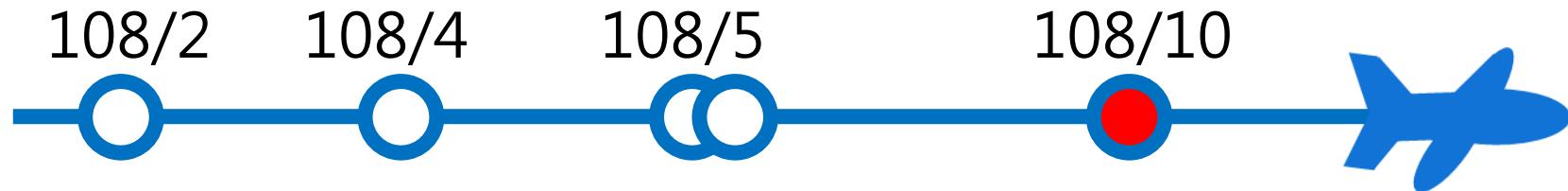
Star 17,889

Add initial exploit for CVE-2019-0708, BlueKeep #12283

bcook-r7 wants to merge 42 commits into rapid7:master from busterb:bluekeep



Adobe Acrobat與Reader弱點



- 108年10月，Adobe之安全性公告指出，Adobe Acrobat與Reader存在越界寫入、使用釋放後記憶體及緩衝區溢位等弱點，攻擊者可藉由誘騙使用者點擊含有惡意程式碼的連結或檔案，進而執行任意程式碼

產品	受影響的版本	建議措施
Acrobat DC與Acrobat Reader DC (Continuous track version)	2019.012.20040(含)以前版本	更新至2019.021.20047以後版本
Acrobat 2017與Acrobat Reader 2017 (Classic 2017 versions)	2017.011.30148(含)以前版本	更新至2017.011.30150以後版本
Acrobat DC與Acrobat Reader DC (Classic 2015 versions)	2015.006.30503(含)以前版本	更新至2015.006.30504以後版本

弱點應變關鍵(1/2)

- 不定期爆發之重大弱點，若未能確實掌握各資通系統的情況並即時因應，將嚴重影響業務之運作，並可能造成機關形象受損
- 機關人員收到廠商、SOC及NCCST的弱點警訊時，**必須經過盤點與清查**，方可得知受影響的主機數量與範圍



受影響主機群

受影響主機群

伺服器主機
與使用者電腦

弱點應變關鍵(2/2)



快速反應

- 如何在弱點發布後，**快速反應**所面臨的威脅與釐清**受影響的版本**



確認範圍

- 如何在確認**受影響版本**後，可確實**掌握受影響範圍**



應變處理

- 如何在確認**受影響範圍**後，**快速因應處理**



事後追蹤

- 如何在因應處理後，持續**追蹤弱點之修補情形**

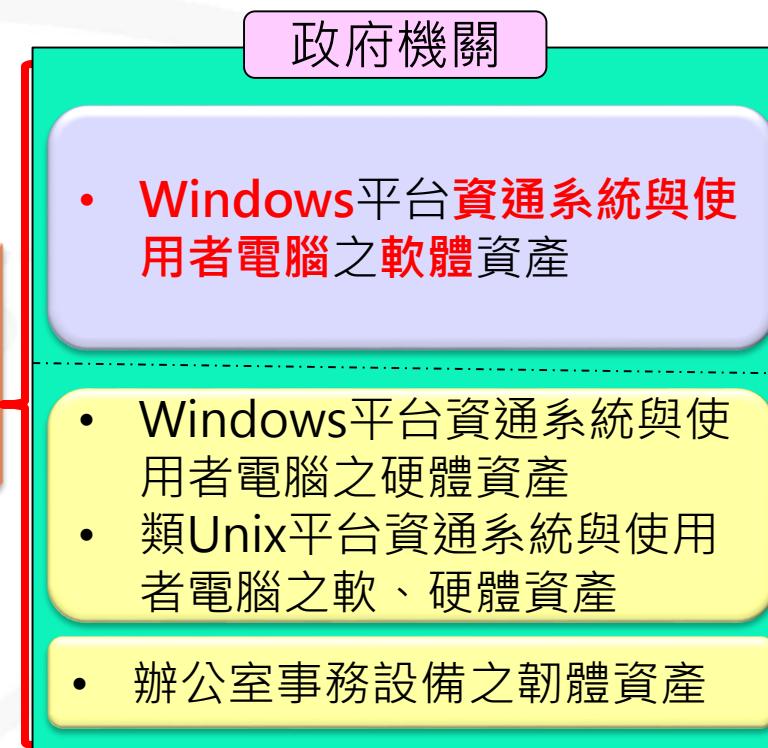
大綱

- 前言
- 政府機關資安弱點通報機制
- 系統功能
- 實作建議
- 後續推動重點

NCCST

資通安全管理法相關規定

- 資通安全管理法第二章第十條
 - 公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施**資通安全維護計畫**
- 資通安全管理法施行細則第六條規範資通安全維護計畫應包含之項目
 - 第六款規範機關應**盤點資通系統**，並標示核心資通系統與相關資產
 - 第七款規範機關應**建立相關風險評估機制**，以針對盤點之資產進行資通安全風險評估



政府機關資安弱點通報機制

- 政府機關資安弱點通報機制(Vulnerability Alert and Notification System, VANS)可協助機關落實資通安
全管理法之資產盤點與風險評估應辦事項，並提供以下服務
 - 透過VANS持續維護資訊資產盤點資料
 - 針對機關登錄的資訊資產項目進行弱點比對，以協助進行系統化風險評估
 - 依照機關訂定的風險值門檻，即時提醒資訊資產風險情形，並進行弱點評估與修補作業
 - 提供微軟安全性更新檢測報告解析功能，協助機關以自動化方式檢視安全性更新落實程度



VANS目標

- 確認資通系統軟體資產弱點
 - 蒐集政府機關使用之軟體資訊，並與國際權威弱點資料庫資訊進行比對，當使用軟體存在重大弱點時，即時得知與應變處理
- 追蹤軟體資產弱點修補情形
 - 追蹤軟體弱點修補情形，並同步進行軟體版本資料更新，以維持資料內容之有效性
- 降低重大弱點管控與追蹤之成本
 - 利用弱點資料庫搭配自動比對方式，提供政府機關相關弱點資訊與自我檢查機制，以降低重大弱點管控與修補情形追蹤所需之人力與資源

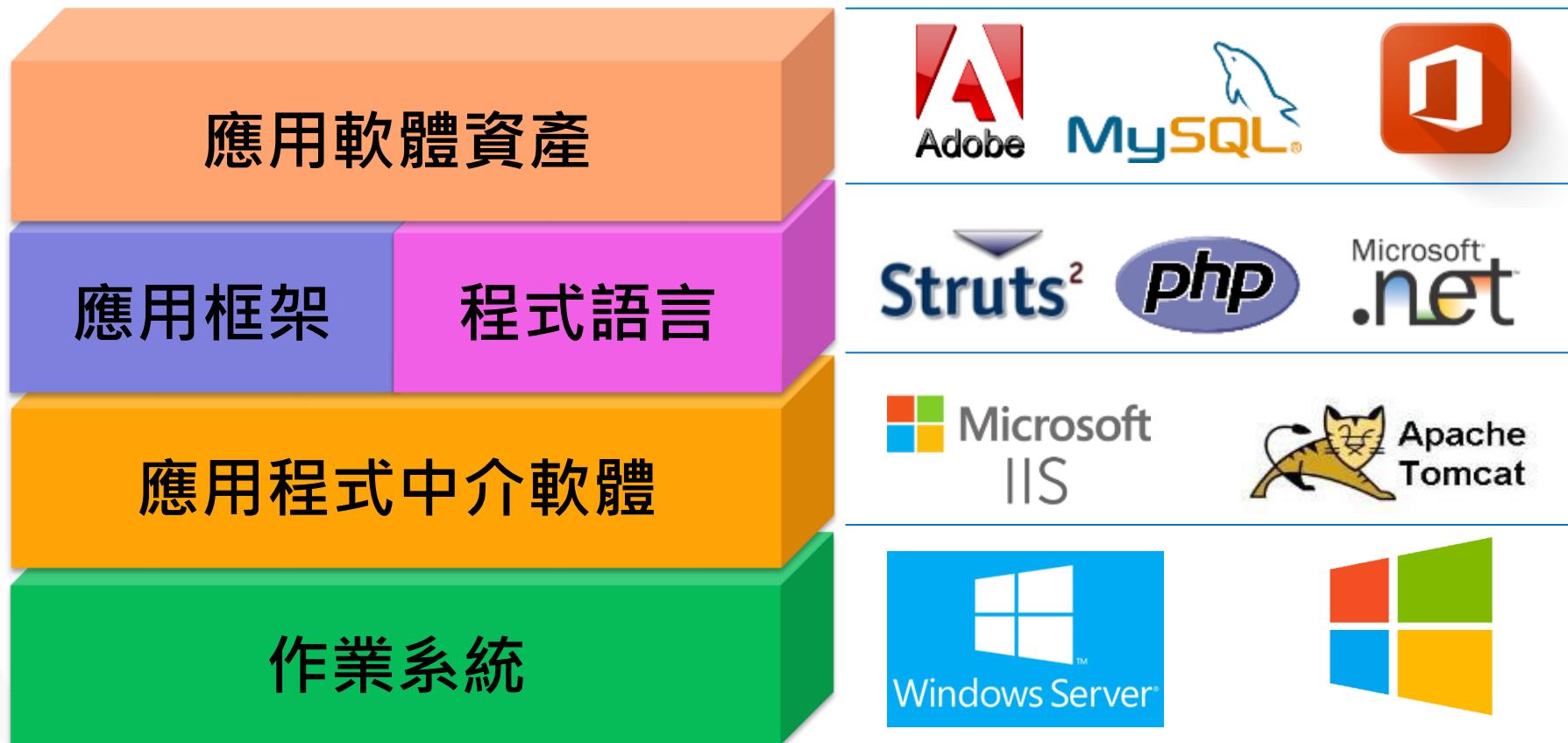
VANS機制介紹(1/2)

- VANS結合資訊資產管理與弱點管理，掌握整體風險情勢，並降低重大弱點爆發時可能造成之損害
 - 定期蒐集主機與電腦所使用之資訊資產項目及版本，建立資訊資產清冊，以達到降低風險與管控成本等目標
 - 將**資訊資產清單與弱點資料庫比對**，以掌握所使用之資訊資產是否存在已公開揭露之弱點資訊



VANS機制介紹(2/2)

- 資訊資產涵蓋範圍

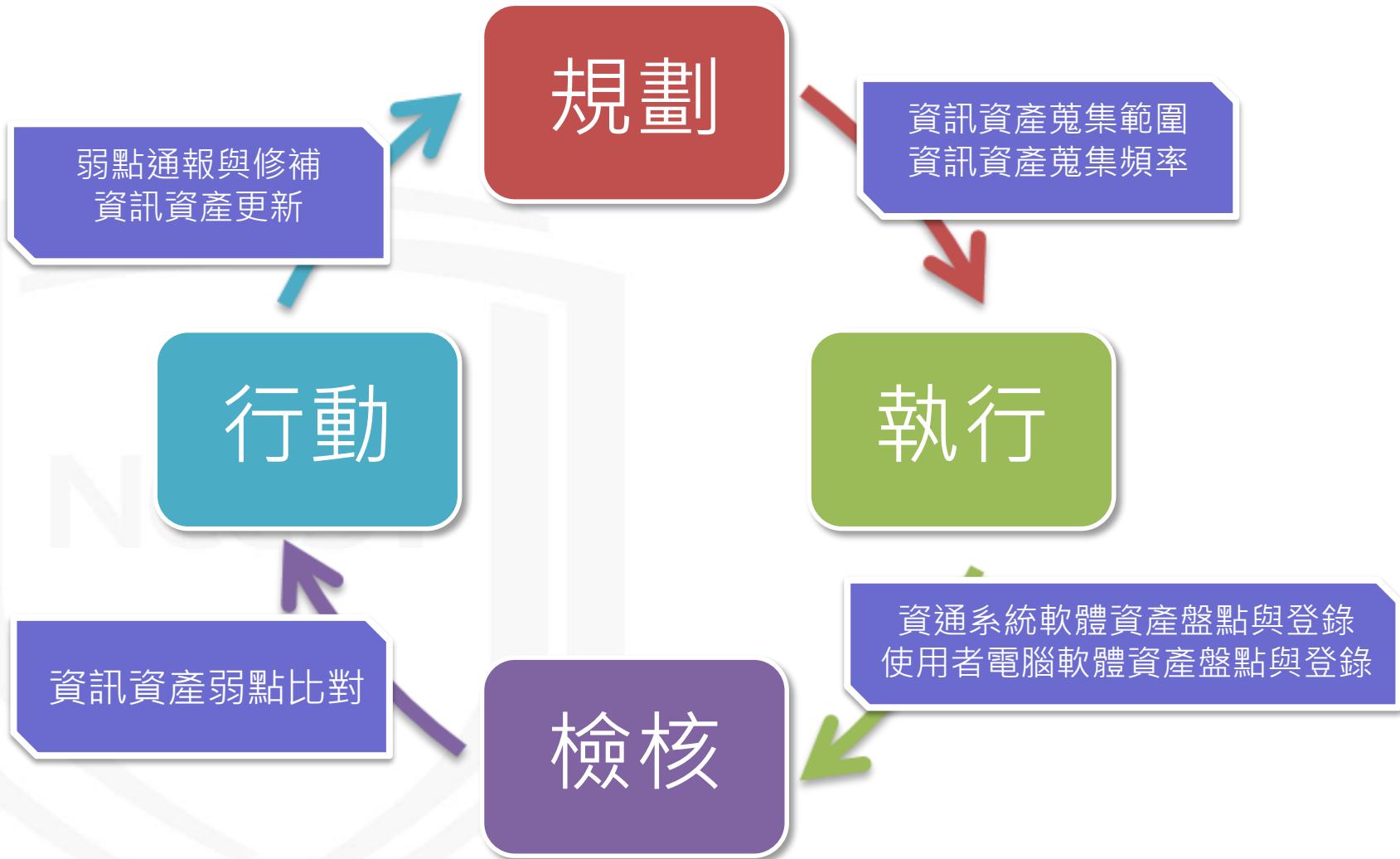


VANS與弱點掃描之差異

- 政府機關大多使用弱掃軟體進行掃描，以釐清是否受弱點影響，以下**比較VANS與弱點掃描之差異**

項目	VANS	弱點掃描
資訊蒐集方式	透過作業系統內建工具或第三方軟體，產出已安裝資訊資產清單	透過網路遠端執行掃描
弱點查詢方式	將登錄至VANS之資訊資產項目與版本進行弱點比對	透過弱掃軟體plugin進行弱點偵測
比對範圍	登錄至VANS之所有資訊資產	目標主機對外服務使用套件
時間性	每10分鐘比對1次	定期執行掃描

VANS機制流程



推動歷程

104年

- 系統開發
- 執行第一階段機關試行專案

105年

- 針對資安責任等級A級機關辦理推廣說明會
- 精進系統功能與服務流程
- 開放資安責任等級A級機關申請使用

106年

- 針對資安責任等級A與B級機關辦理推廣說明會
- 執行第二階段機關試行專案
- 開放資安責任等級A與B級機關申請使用

107年

- 針對資安責任等級A與B級機關辦理推廣說明會
- 執行2次資安服務團專案，於輔導課程推廣本機制，並於實地輔導作業協助2個機關導入本機制
- 與6家國內資產管理廠商洽談合作事宜

108年

- 為提升公務機關辦公場所資安防護能力，擴增盤點範圍與資產蒐集內容
- 配合資安服務團實地輔導辦理試行導入
- 辦理2場次推廣說明會
- 規劃資料介接格式，供廠商進行軟體與VANS間之資料介接

大綱

- 前言
- 政府機關資系弱點通報機制
- 系統功能
- 實作建議
- 後續推動重點

系統介紹

- VANS提供機關登錄資訊資產，藉由系統自動與國際權威弱點資料庫(NVD)比對，羅列出資訊資產之弱點，俾利機關掌握可能面臨之資安風險，以強化資訊資產之資安管理
- 資訊資產盤點標的包含資通系統與使用者電腦之軟體資訊，協助機關掌握資訊資產潛在弱點



NVD

CVE
cve.mitre.org

CPE
common platform enumeration

政府機關資通系統弱點通報機制 (VANS)

一般帳號登入 管理者帳號登入

iAuth管理帳號

個人帳號

密碼

登入 申請個人帳號 忘記密碼



資訊資產格式

- 資通系統與使用者電腦組成多變，所用之軟體套件多樣，難有資產管理系統能提供一體適用之軟體套件蒐集方式
- 不同廠商針對同一軟體資產，可能有不同的描述方式



資訊資產呈現方式(1/2)

- Common Platform Enumeration(簡稱CPE)，為美國國家標準技術研究所(NIST)所提出標準化方式，用以描述與識別企業內的應用程式、作業系統及硬體設備等資訊資產，最新版本為2.3
- CPE條目格式
 - 主要分為三大類：作業系統(o)、應用程式(a)及硬體(h)
 - 主要資訊：廠商名稱(vendor)、產品名稱(product)、產品版本(version)、產品更新(update)、產品版次(edition)、語系(language)

資訊資產呈現方式(2/2)

- CPE條目範例

- Windows Server 2008 R2 Service Pack 1 64位元

廠商名稱	版本	版次
➤ cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:x64:.*.*.*.*		

產品類別 產品名稱 更新

- Oracle JDK 1.8.0 Update 92

廠商名稱	版本
➤ cpe:2.3:a:oracle:jdk:1.8.0:update_92:.*.*.*.*	

產品類別 產品名稱 更新

弱點呈現方式

- Common Vulnerabilities and Exposures(簡稱CVE)羅列各種資安弱點，並給予編號以便查閱
- CVE目標為將所有已知弱點與資安風險的名稱標準化，俾利於各個弱點資料庫與安全工具之間發布資料
- 現由美國非營利組織MITRE所屬的National Cybersecurity FFRDC負責營運維護
- 每一個CVE都賦予一個專屬的編號，格式如下
 - CVE-**YYYY**-**NNNN**

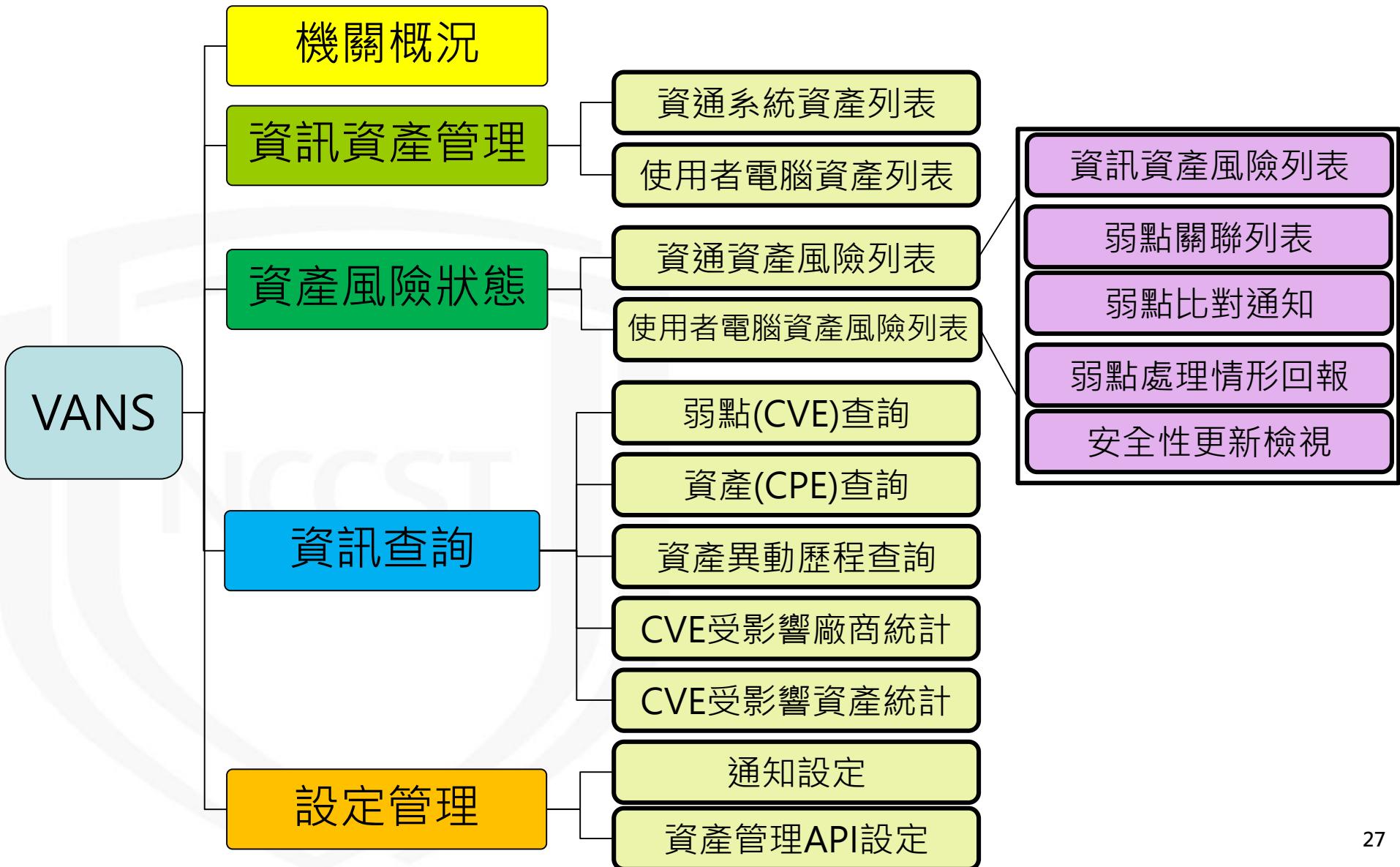
西元紀年 流水號



弱點資料庫

- National Vulnerability Database(簡稱NVD)為NIST所建置，專門用來蒐集各種資通系統弱點資訊的資料庫網站
 - 自MITRE取得CVE列表，並增加修補建議連結、嚴重性評分(CVSS分數)及影響等級等資訊
 - 建立CPE與CVE對應關係，以解決弱點與資訊資產之對應關係
 - 目前已有150,148筆弱點數量與396,268筆CPE數量
 - VANS系統每天更新1次弱點

系統功能概要說明



功能介紹-介面說明

系統名稱

政府機關資安弱點通報機制

測試人員

機關概況

資訊資產管理

資產風險狀態

資訊查詢

設定管理

功能選單列

登出

系統名稱

政府機關資安弱點通報機制

測試人員

機關概況

資訊資產管理

資產風險狀態

資訊查詢

設定管理

功能路徑

主畫面

檢視方式
資通系統 使用者電腦

資通系統資產類別統計

類別	數量	百分比
使用者電腦	555	99.6%
資通系統	25	0.4%

資通系統弱點處理情形(CVE)

狀態	數量	百分比
已處理	328	95.6%
未處理	55	4.4%

資通系統安全性更新情形(Windows Update)

狀態	數量	百分比
已更新	7	100.0%
未更新	0	0.0%

檢視方式
資通系統 使用者電腦

資通系統資產類別統計

類別	數量	百分比
使用者電腦	555	99.6%
資通系統	25	0.4%

資通系統弱點處理情形(CVE)

狀態	數量	百分比
已處理	328	95.6%
未處理	55	4.4%

資通系統安全性更新情形(Windows Update)

狀態	數量	百分比
已更新	7	100.0%
未更新	0	0.0%

功能介紹-資產管理(1/6)

● 系統化管理資訊資產

- 提供機關以系統化方式管理Windows平台資通系統與使用者電腦之軟體資產



機關概況

資訊資產管理

資訊資產管理 > 資通系統資產列表

資訊資產管理 > 使用者電腦資產列表

資產風險狀態

資訊查詢

設定管理

資訊資產管理 > 資通系統資產列表

完整軟體資產CPE清單下載 常見重要軟體資產CPE清單下載 下載上傳檔案格式範本 資產清單上傳

資通系統資產清單下載 資產關聯更新CPE清單下載 資通系統資產清單匯出(PDF)

新增資產

測試帳號1

資訊

資訊資產管理 > 使用者電腦資產列表

完整軟體資產CPE清單下載 常見重要軟體資產CPE清單下載 下載上傳檔案格式範本 資產清單上傳

使用者電腦資產清單下載 資產關聯更新CPE清單下載 使用者電腦資產清單匯出(PDF)

新增資產

測試帳號1

資訊

資產名稱	資產廠商	資產版本	CPE2.3	資產數量	編輯	刪除
HP Array Configuration Utility	Hewlett-Packard Development Company, L.P.	8.30.5.0	cpe:2.3:adhp:array_configuration_utility:8.30.5.0:*****	2		
Heartleaf Server Rancho/Unidata	Hewlett-Packard	1.0.0.0	cpe:2.3:adhp:heartleaf_server_rancho/unidata:1.0.0.0:*****	2		

10

10

29

功能介紹-資產管理(2/6)



• 資產CPE清單下載

- 提供軟體資產CPE清單下載，可運用此清單進行CPE條目查詢與對應

資訊資產管理 > 資通系統資產列表

測試帳號1

完整軟體資產CPE清單下載 常見重要軟體資產CPE清單下載 下載上傳檔案格式範本 資產清單上傳

資通系統資產清單下載 資產關聯更新CPE清單下載 資通系統資產清單匯出(PDF)

新增資產

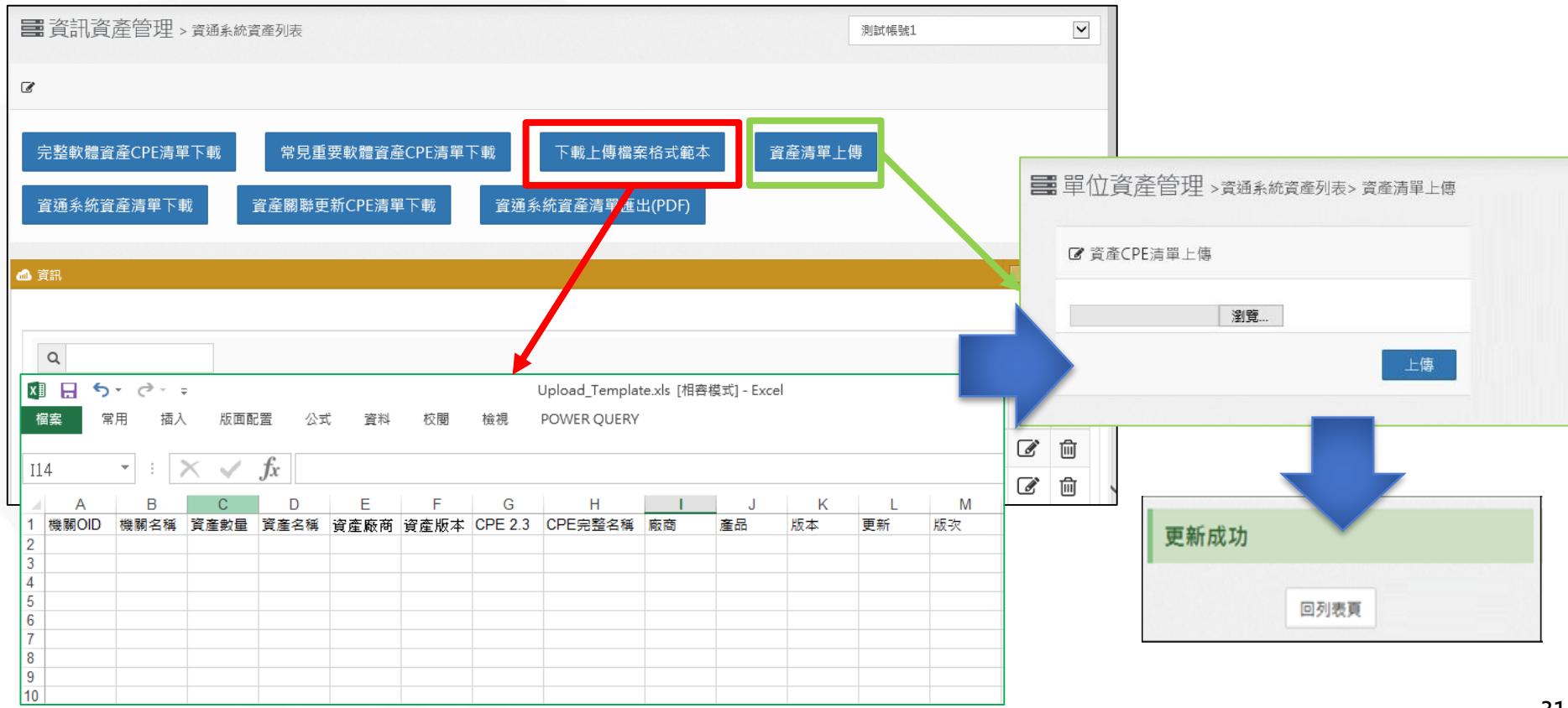
資產名稱	A	B	C	D	E	F	G	H	I	J	K	
	1	勾選	機關OID	機關名稱	資產數量	CPE 2.3	CPE完整名稱	廠商	產品	版本	更新	版次
Adobe Acrobat XI Standard	2265					cpe:2.3:o:microsoft:windows_10:-.*.*.*.*:x64.*	Microsoft Windows 10 64-bit	microsoft	windows_10	-	*	*
	2266					cpe:2.3:o:microsoft:windows_10:-.*.*.*.*:x86.*	Microsoft Windows 10 32-bit	microsoft	windows_10	-	*	*
Adobe Acrobat DC	2267					cpe:2.3:o:microsoft:windows_10:1511.*.*.*.*:x64.*	Microsoft Windows 10 1511 64-bit	microsoft	windows_10	1511	*	*
	2268					cpe:2.3:o:microsoft:windows_10:1511.*.*.*.*:x86.*	Microsoft Windows 10 1511 32-bit	microsoft	windows_10	1511	*	*
	2269					cpe:2.3:o:microsoft:windows_10:1607.*.*.*.*:x86.*	Microsoft Windows 10 1607 32-bit	microsoft	windows_10	1607	*	*
	2270					cpe:2.3:o:microsoft:windows_10:1607.*.*.*.*:x64.*	Microsoft Windows 10 1607 64-bit	microsoft	windows_10	1607	*	*
	2271					cpe:2.3:o:microsoft:windows_10:1703.*.*.*.*:x64.*	Microsoft Windows 10 1703 64-bit	microsoft	windows_10	1703	*	*
	2272					cpe:2.3:o:microsoft:windows_10:1703.*.*.*.*:x86.*	Microsoft Windows 10 1703	microsoft	windows_10	1703	*	*
	2273					cpe:2.3:o:microsoft:windows_10:1709.*.*.*.*:x64.*	Microsoft Windows 10 1709 64-bit	microsoft	windows_10	1709	*	*
	2274					cpe:2.3:o:microsoft:windows_10:1709.*.*.*.*:x86.*	Microsoft Windows 10 1709	microsoft	windows_10	1709	*	*
	2275					cpe:2.3:o:microsoft:windows_10:1803.*.*.*.*:x64.*	Microsoft Windows 10 1803 on x64	microsoft	windows_10	1803	*	*
	2276					cpe:2.3:o:microsoft:windows_10:1803.*.*.*.*:x86.*	Microsoft Windows 10 1803	microsoft	windows_10	1803	*	*
	2277					cpe:2.3:o:microsoft:windows_10:1809.*.*.*.*:x64.*	Microsoft Windows 10 1809 on x64	microsoft	windows_10	1809	*	*
	2278					cpe:2.3:o:microsoft:windows_10:1809.*.*.*.*:arm64.*	Microsoft Windows 10 1809 on ARM64	microsoft	windows_10	1809	*	*
	2279					cpe:2.3:o:microsoft:windows_10:1809.*.*.*.*:x86.*	Microsoft Windows 10 1809	microsoft	windows_10	1809	*	*
	2280					cpe:2.3:o:microsoft:windows_10:1903.*.*.*.*:x64.*	Microsoft Windows 10 1903 64-bit	microsoft	windows_10	1903	*	*

作業系統 應用程式或網站伺服器 程式語言執行環境 開發框架 網站採用第三方元件 資料庫

功能介紹-資產管理(3/6)

- 透過上傳檔案格式範本登錄資訊資產
 - 可同時填寫常見資產格式與CPE格式之資訊資產，並於完成後上傳至VANS系統，以進行資訊資產登錄

Screenshot illustrating the process of uploading asset information using a template:



The process involves:

- Download the "Upload Template" (highlighted with a red box).
- Open the Excel template file (`Upload_Template.xls`).
- Fill in the asset information according to the template columns.
- Click the "Asset List Upload" button (highlighted with a green box) to open the upload dialog.
- Upload the completed Excel file via the "Browse..." button.
- Click the "Upload" button in the dialog.
- Wait for the "Success" message ("更新成功") to appear.

功能介紹-資產管理(4/6)



• 資訊資產清單下載

- 下載已登錄至VANS系統之資訊資產，以利進行資料留存或後續資產更新作業

資訊資產管理 > 資通系統資產列表

測試帳號1

完整軟體資產CPE清單下載 常見重要軟體資產CPE清單下載 下載上傳檔案格式範本 資產清單上傳

資通系統資產清單下載 資產關聯更新CPE清單下載 資通系統資產清單匯出(PDF)

資訊

新增資產

10

default-cpe-test-Asset-download (1).xls [相容模式] - Excel

檔案 常用 版面配置 公式 資料 校閱 檢視 POWER QUERY

N17

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	機關OID	機關名稱	資產數量	資產名稱	資產廠商	資產版本	CPE 2.3	CPE 完整名稱	廠商	產品	版本	更新	版次
2	test	測試帳號1	143	silverstripe	silverstripe	2.4.10	cpe:2.3:a:silverstripe:silverstripe:2.4.10-**: SilverStripe 2.4.10	silverstripe	silverstripe	2.4.10	*	*	
3	test	測試帳號1	154	apache	wicket	6.0.0-beta	cpe:2.3:a:apache:wicket:6.0.0-beta1-**: Apache Software Foundation Wicket 6.0.0-beta1	apache	wicket	6.0.0-beta	*	*	
4	test	測試帳號1	165	apache	hadoop	3.0.0	cpe:2.3:a:apache:hadoop:3.0.0.alpha4-**: Apache Software Foundation Hadoop 3.0.0 Alpha4	apache	hadoop	3.0.0	alpha4	*	
5	test	測試帳號1	44	microsoft	windows_server_2008	-	cpe:2.3:o:microsoft:windows_server_2008:- Microsoft Windows Server 2008 Service Pack 1	microsoft	windows_server_2008	-	sp2	*	
6	test	測試帳號1	55	microsoft	windows_server_2016	1803	cpe:2.3:o:microsoft:windows_server_2016:- Microsoft Windows Server 2016 1803	microsoft	windows_server_2016	1803	*	*	
7	test	測試帳號1	66	microsoft	windows_server_2019	-	cpe:2.3:o:microsoft:windows_server_2019:- Microsoft Windows Server 2019	microsoft	windows_server_2019	-	*	*	
8	test	測試帳號1	77	microsoft	windows_7	-	cpe:2.3:o:microsoft:windows_7-**: ultime Microsoft Windows 7 Ultimate Edition on x86	microsoft	windows_7	-	-	*	

功能介紹-資產管理(5/6)

● 資產名單匯出(PDF)

– 將已登錄VANS系統之資訊資產以PDF格式匯出，可進行資料留存與備查

資訊資產管理 > 資通系統資產列表

完整軟體資產CPE清單下載 常見重要軟體資產CPE清單下載 下載上傳檔案格式範本 資產清單上傳

資通系統資產清單下載 資產關聯更新CPE清單下載 **資通系統資產清單匯出(PDF)**

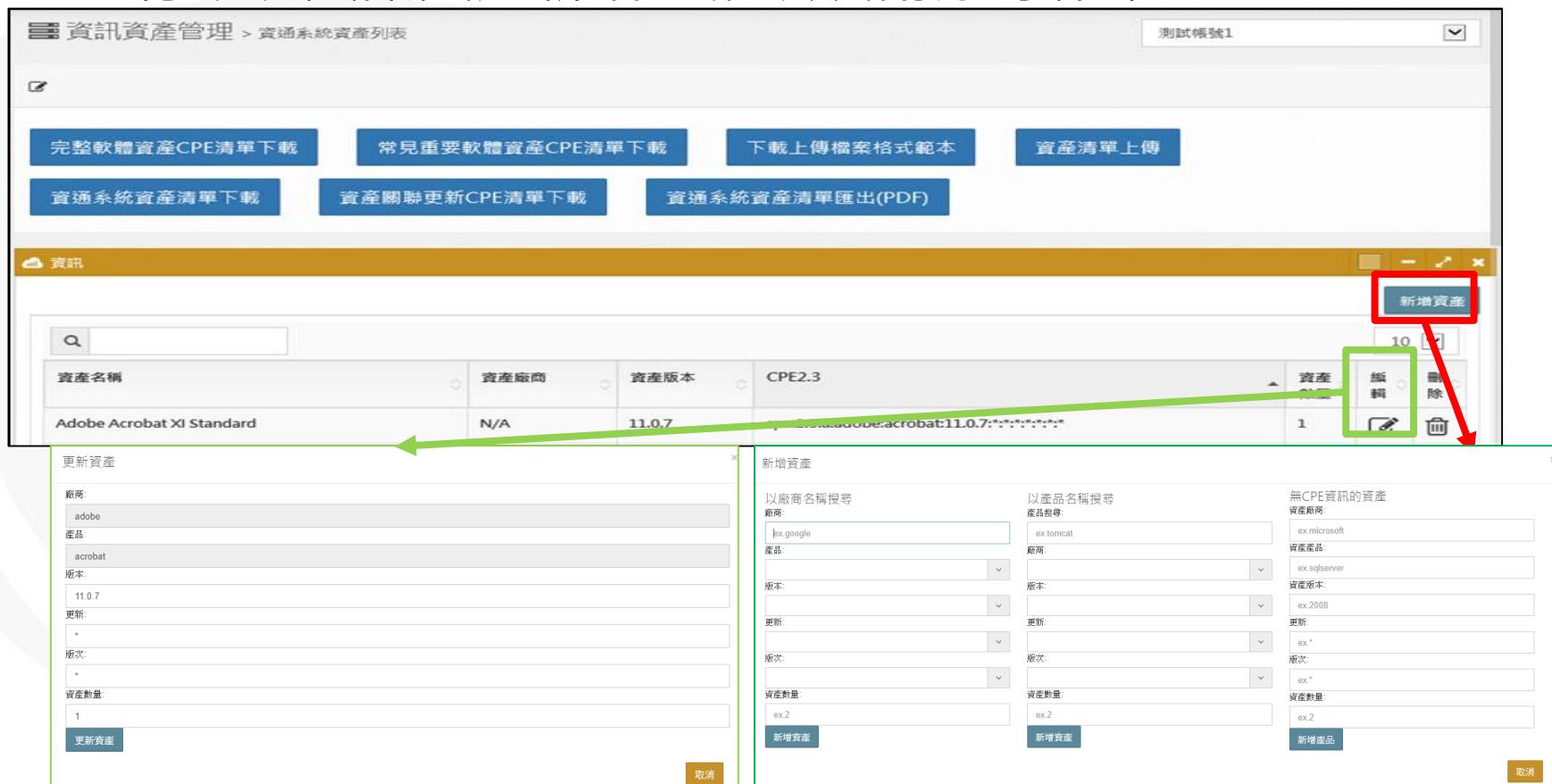
測試帳號1

機關OID	機關名稱	資產數量	資產名稱	資產廠商	資產版本	CPE完整名稱	廠商	產品	版本	更新	版次
test	測試帳號1	143	N/A	N/A	N/A	cpe:2.3:a:silverstripe:cms:2.4.10	silverstripe	silverstripe	2.4.10	*	*
test	測試帳號1	154	N/A	N/A	N/A	cpe:2.3:a:apache:tomcat:6.0.0-beta1	apache	wicket	6.0.0-beta1	*	*
test	測試帳號1	165	N/A	N/A	N/A	cpe:2.3:a:apache:hadoop:3.0.0-alpha4	apache	hadoop	3.0.0	alpha4	*
test	測試帳號1	44	N/A	N/A	N/A	cpe:2.3:o:microsoft:windows_server_2008_r2_sp2:standard:x86_*	microsoft	windows_server_2008	-	sp2	*
test	測試帳號1	55	N/A	N/A	N/A	cpe:2.3:o:microsoft:windows_server_2016:1803:*	microsoft	windows_server_2016	1803	*	*

功能介紹-資產管理(6/6)

● 編輯資訊資產

– 除透過CPE清單批次更新資產外，亦可透過網頁頁面進行單項資訊資產新增、修改及刪除等作業



The screenshot shows the '資產資訊管理 > 資通系統資產列表' page. At the top, there are several download and upload buttons:

- 完整軟體資產CPE清單下載
- 常見重要軟體資產CPE清單下載
- 下載上傳檔案格式範本
- 資產清單上傳
- 資通系統資產清單下載
- 資產關聯更新CPE清單下載
- 資通系統資產清單匯出(PDF)

In the center, a table lists assets. A green arrow points from the '更新資產' button in the 'Actions' column of the table to the '更新資產' dialog box at the bottom left. Another green box highlights the '編輯' (Edit) button in the same column. A red box highlights the '新增資產' (Add Asset) button in the 'Actions' column of the table, with a red arrow pointing to the '新增資產' dialog box at the bottom right.

更新資產 Dialog Box (Left):

- 廠商: adobe
- 產品: acrobat
- 版本: 11.0.7
- 更新: *
- 版次: *
- 資產數量: 1
- 新增資產

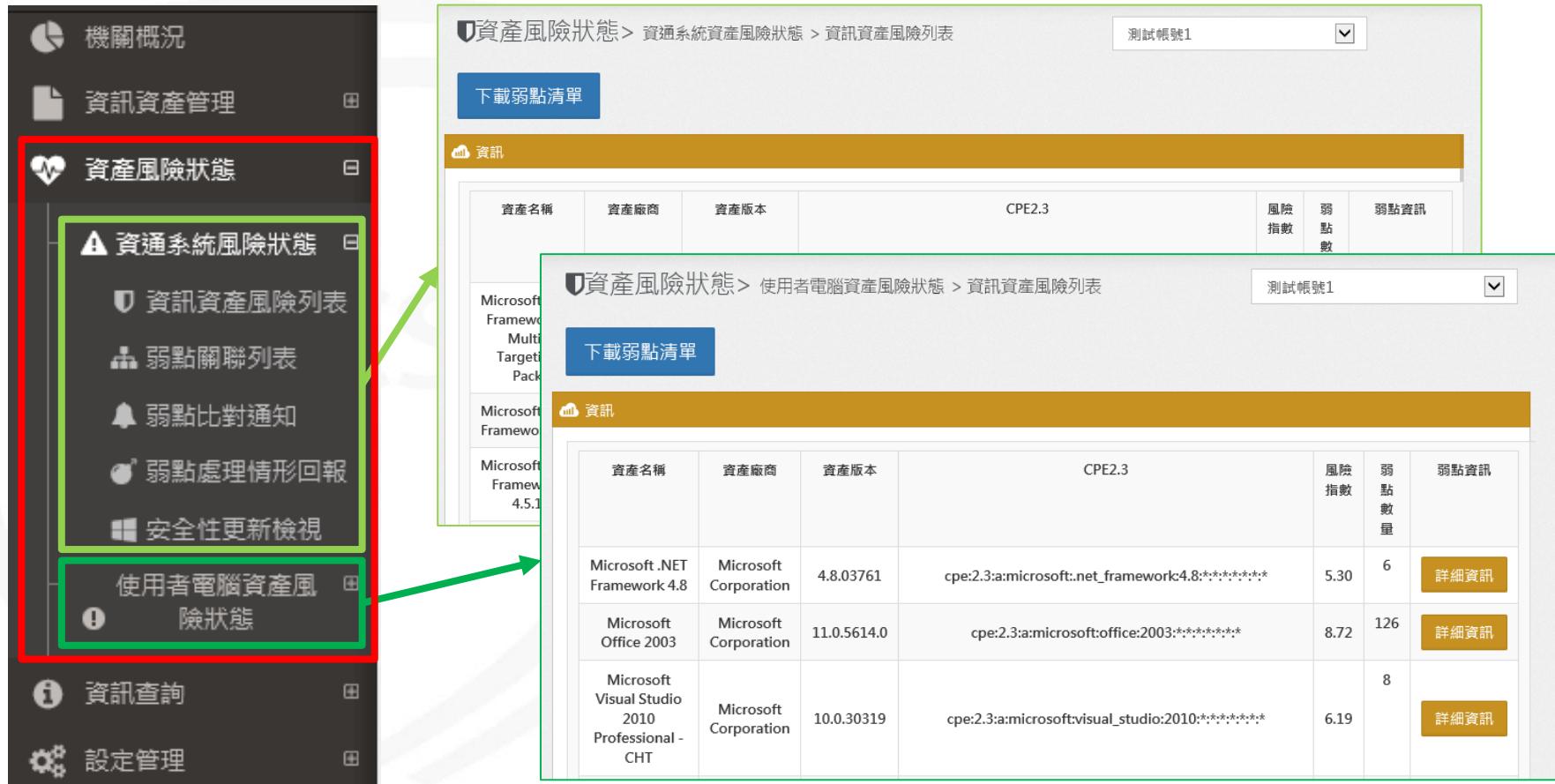
新增資產 Dialog Box (Right):

- 以廠商名稱搜尋
廠商: lex.google
- 以產品名稱搜尋
產品: ex.tomcat
- 無CPE資訊的資產
資產廠商: ex.microsoft
- 資產產品: ex.sqlserver
- 資產版本: ex.2008
- 更新: ex.*
- 版次: ex.*
- 資產數量: ex.2
- 新增資產

功能介紹-風險管理(1/5)

● 自動化比對資訊資產弱點

– VANS系統將已登錄之資訊資產項目與NVD弱點資料庫自動比對，並顯示弱點比對結果



The screenshot illustrates the VANS system's Asset Risk Status module. On the left, a sidebar menu lists various management functions. The 'Asset Risk Status' section is highlighted with a red border, and the 'Information Asset Risk List' item within it is highlighted with a green border. Two green arrows point from this highlighted area to two separate windows on the right, each displaying a table of comparison results.

Top Right Window (Information Asset Risk List):

資產名稱	資產廠商	資產版本	CPE2.3	風險指數	弱點數	弱點資訊
Microsoft Framework Multi Target Pack	Microsoft		cpe:2.3:a:microsoft:multi-target-pack:1.0	6.00	6	詳細資訊
Microsoft Framework 4.5.1	Microsoft		cpe:2.3:a:microsoft:framework-4.5.1:1.0	6.00	6	詳細資訊

Bottom Right Window (User Computer Asset Risk Status):

資產名稱	資產廠商	資產版本	CPE2.3	風險指數	弱點數量	弱點資訊
Microsoft .NET Framework 4.8	Microsoft Corporation	4.8.03761	cpe:2.3:a:microsoft:.net_framework:4.8.*.*.*.*.*	5.30	6	詳細資訊
Microsoft Office 2003	Microsoft Corporation	11.0.5614.0	cpe:2.3:a:microsoft:office:2003.*.*.*.*.*	8.72	126	詳細資訊
Microsoft Visual Studio 2010 Professional - CHT	Microsoft Corporation	10.0.30319	cpe:2.3:a:microsoft:visual_studio:2010.*.*.*.*.*	6.19	8	詳細資訊

功能介紹-風險管理(2/5)

- 檢視資訊資產弱點並填寫改善措施

– 可檢視資訊資產存在之CVE弱點資訊與CVSS分數，並可針對各CVE弱點填寫改善措施



機關概況

資訊資產管理

資產風險狀態

資通系統風險狀態

資訊資產風險列表 (highlighted with a red box)

弱點關聯列表

弱點比對通知

弱點處理情形回報

安全性更新檢視

使用者電腦資產風險狀態

資訊查詢

設定管理

資產風險狀態 > 資通系統資產風險狀態 > 資訊資產風險列表

測試帳號1

下載弱點清單

修改改善措施

請勿使用 >,<, &, " 或 ' 字元填寫改善措施

確定修改

詳細資訊

CVE編號 CVSS 發布時間 更新時間 改善措施

CVE-2010-3228	9.3	2010-10-13 15:00:45	2019-02-26 09:04:00	已填寫改善措施, 查看詳情
CVE-2010-3332	5	2010-09-22 15:00:06	2018-10-12 17:58:32	已填寫改善措施, 查看詳情

功能介紹-風險管理(3/5)

● 弱點關聯列表

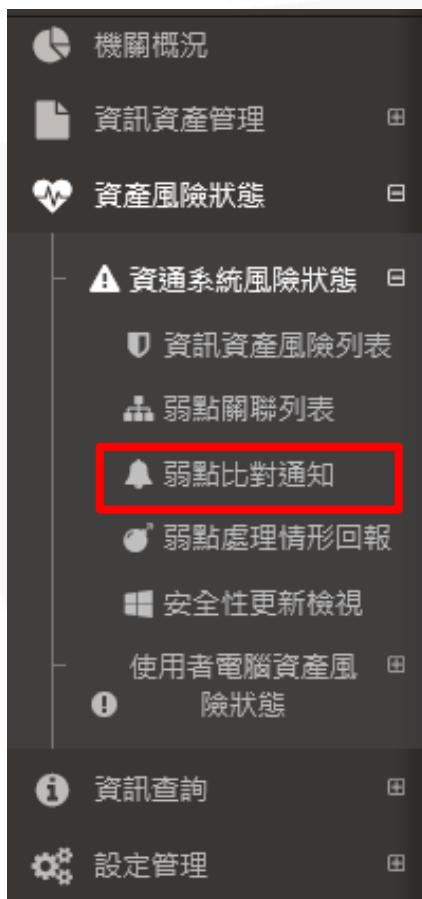
— 設定時間區間，並檢視各弱點影響之資訊資產

-  機關概況
-  資訊資產管理
-  資產風險狀態
-  資通系統風險狀態
-  資訊資產風險列表
-  弱點關聯列表
-  弱點比對通知
-  弱點處理情形回報
-  安全性更新檢視
-  使用者電腦資產風險狀態
-  資訊查詢
-  設定管理

資產風險狀態 > 資通系統資產風險狀態 > 弱點關聯列表					測試帳號1
起始時間	2019-10-23	結束時間	2019-11-23	查詢	
資訊					
CVE-2018-9549	CVSS Score: 9.3	發布時間: 2018-12-06 09:29:01	更新時間: 2019-11-14 12:11:00		
N/A	N/A	N/A	cpe:2.3:o:google:android:7.1.2:*****:**	2019-11-17 12:25:39	比對時間
CVE-2018-9553	CVSS Score: 9.3	發布時間: 2018-12-06 09:29:01	更新時間: 2019-11-14 12:11:00		
N/A	N/A	N/A	cpe:2.3:o:google:android:7.1.2:*****:**	2019-11-17 12:25:39	比對時間
CVE-2018-9555	CVSS Score: 8.3	發布時間: 2018-12-06 09:29:01	更新時間: 2019-11-14 12:11:00		
N/A	N/A	N/A	cpe:2.3:o:google:android:7.1.2:*****:**	2019-11-17 12:25:39	比對時間

功能介紹-風險管理(4/5)

- 系統會依CVSS分數門檻寄發通知信
- 同一個資產的同一弱點只會於首次比對時進行1次通知，以後不會再出現相同的弱點通知



【VANS】資訊資產風險項目通知

收件者: ...
簽名者: vans@nccst.nat.gov.tw

敬啟者 您好：

此為「政府機關資安弱點通報機制」之通知郵件。

貴機關之所以收到此通知信件，在於貴機關於 VANS 系統所登錄之資訊資產，經過系統比對弱點資料庫後，發現存有風險項目，建議貴機關對資訊資產風險進行修補，以避免資安風險。修補作業完成後，再煩請貴機關至 VANS 系統進行資訊更新，以協助本中心掌握修補情況。
謝謝。

VANS 系統網頁連結：
<https://vans.nccst.nat.gov>

如有任何疑問，請聯絡我司。
聯絡電話：(02)6631-645

資產風險狀態 > 資通系統資產風險狀態 > 弱點比對通知

弱點通知列表

通知時間	資產數量	弱點數量	詳細資訊	通知顯示	匯出勾選弱點通知	全選
2019-11-17 00:37:17	1	171	開啟	ON <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2019-11-08 16:39:21	28	456	開啟	ON <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Showing 1 to 2 of 2 entries

Previous **1** Next

功能介紹-風險管理(5/5)

● 弱點處理情形回報

– 查看機關受影響之各項弱點詳細資訊，並針對須回報之弱點選擇處理方式



* 資產風險狀態 > 資通系統資產風險狀態> 弱點處理情形回報

弱點編號
弱點編號

開始時間*
2019-09-29

結束時間*
2019-10-29

弱點狀態*
All

弱點編號	CVSS Score	發布時間	更新時間	詳細資訊
CVE-2019-1226	10.0	2019/08/15 06:15:18	2019/10/11 09:10:00	詳細資訊
CVE-2019-1222	10.0	2019/08/15 06:15:18	2019/10/11 09:10:00	詳細資訊
CVE-2019-1182	10.0	2019/08/15 06:15:16	2019/10/11 09:10:00	詳細資訊

CVE資訊

CVE-2019-1226 CWE-284

Summary

NVD官網弱點說明連結
<https://nvd.nist.gov/vuln/detail/CVE-2019-1226>

相關新聞

MISC
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1226>

CONFIRM
<http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190819-01-windows-en>

CONFIRM
<https://cert-portal.siemens.com/productcert/pdf/ssa-187667.pdf>

CVSS Score: 10

Access Vector: LOW
AccessComplexity: NETWORK
AccessVector: NONE
Authentication: NONE

CVSS影響評估

Availability/Impact: COMPLETE
Confidentiality/Impact: COMPLETE
Integrity/Impact: COMPLETE

詳細資訊

cpe:2.3:o:microsoft:windows_server_2016:1803:*****
cpe:2.3:o:microsoft:windows_10:1903:*****x64:*

功能介紹-安全性更新檢視(1/4)

- 半自動化彙整安全性更新報表

- 將多份MBSACLI安全性更新檢測結果報告(.xml)壓縮並上傳至VANS系統，可協助解析並顯示彙整結果



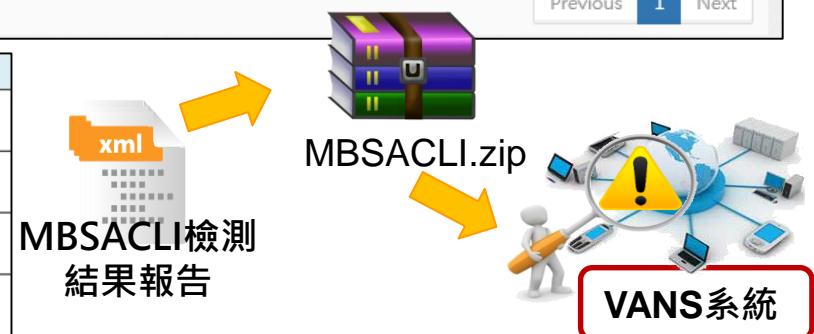
資產風險狀態 > 資通系統資產風險狀態> 安全性更新檢視

專案列表

狀態	專案名稱	安全性更新率	專案建立時間	壓縮檔總數	已更新電腦數	xml總數	檢視報告	新增壓縮檔	編輯專案名稱	刪除
✓	1081022	0.00 %	2019-10-22 10:12:48	1	0	7				
✓	project	39.29 %	2019-06-19 09:10:44	1	55	140				

Showing 1 to 2 of 2 entries

狀態	說明
	正在解析MBSACLI檢測結果
✓	解析完成，檔案無誤
!	解析完成，檔案有誤：有重複檔名的XML報告
✗	解析完成，檔案有誤：請確認「壓縮檔總數」與「xml總數」內的錯誤訊息



功能介紹-安全性更新檢視(2/4)

- 「檢視報告」功能呈現各電腦的MBSACLI檢測結果
 - 點選後將跳轉至「電腦更新情形列表」，顯示各電腦缺漏安全性更新列表
 - 點選「安全性更新說明連結」，將連至Microsoft該安全性更新說明網頁

資產風險狀態 > 資通系統資產風險狀態 > 安全性更新檢視

專案列表

狀態	專案名稱	安全性更新率	專案建立時間	壓縮檔總數	已更新電腦數	xml總數	檢視報告	新增壓縮檔	編輯專案名稱	刪除
	project	0.00 %	2019-10-22 10:12:48	1	0	7				
	test	39.29 %	2019-06-19 09:10:44	1	55	140				

Showing 1 to 2 of 2 entries

Previous 1 Next

資產風險狀態 > 資通系統資產風險狀態 > 安全性更新檢視 > 同伺服器主機更新情形列表

專案名稱: project
results_WIN7-R-0006

KBID	安全性更新類別	安全性更新名稱	MS公告號碼	是否安裝	Severity	安全性更新說明連結
890830	Windows	Windows Malicious Software Removal Tool x64 - June 2017 (KB890830)	N/A	false	0	http://support.microsoft.com/kb/890830
2479943	Windows	Security Update for Windows 7 for x64-based Systems (KB2479943)	MS11-015	false	0	http://go.microsoft.com/fwlink/?LinkId=207841

Microsoft

使用 Windows 惡意軟體移除工具移除特定的常見惡意程式

摘要

Windows 惡意軟體移除工具 (MSRT) 可協助移除執行 Windows 10、Windows 8.1、Windows Server 2012 R2、Windows 8、Windows Server 2012、Windows 7 或 Windows Server 2008 的電腦中的惡意軟體。

Microsoft 通常每月發行 MSRT (做為 Windows Update 的一部分或做為單獨的工具)。使用此工具可尋找和移除特定的常見威脅，並恢復其進行的變更 (請參閱所覆蓋的威脅)。如

功能介紹-安全性更新檢視(3/4)

- 於電腦更新情形列表點選「**缺漏安全性更新查詢列表**」按鈕，可檢視各安全性更新分別有哪些電腦有缺漏更新
 - 點選「**安全性更新說明連結**」，將連至Microsoft該安全性更新說明網頁

資產風險狀態 > 資通系統資產風險狀態 > 安全性更新檢視 > 伺服器主機更新情形列表

專案名稱: project
results_WIN7-R-0006

搜尋

KBID	安全性更新類別	安全性更新名稱	MS公告號碼	是否安裝	Severity	安全性更新說明連結
------	---------	---------	--------	------	----------	-----------

返回專案列表 缺漏安全性更新查詢列表 10

Microsoft

適用於 Windows 7 SP1 和 Windows Server 2008 R2 SP1 之 .NET Framework 3.5.1、4.5.2、4.6、4.6.1、4.6.2 和 4.7 的僅限安全性更新：2017 年 9 月 12 日

適用於：Microsoft .NET Framework 4.7, Microsoft .NET Framework 4.6.2, Microsoft .NET Framework 4.6.1, 更多

[檢視本文適用的產品。](#)

摘要

此安全性更新能解決 Microsoft .NET Framework 中的弱點，此弱點可能會在 Microsoft .NET Framework 處理未受信任的輸入時允許遠端執行程式碼。成功在軟體中使用 .NET Framework 來利用

資產風險狀態 > 資通系統資產風險狀態 > 安全性更新檢視 > 缺漏安全性更新查詢列表

專案名稱: project

搜尋

KBID	安全性更新類別	安全性更新名稱	MS公告號碼	是否安裝	Severity	安全性更新說明連結
4041090	Windows	2017-09 Security Only Update for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7 on Windows 7 and Server 2008 R2 for x64 (KB4041090)	N/A	false	3	http://support.microsoft.com/kb/4041090

缺漏本更新之報告名稱：

results_WIN7-R-0007 results_WIN7-R-0003

缺漏更新電腦列表

功能介紹-安全性更新檢視(4/4)

- 若需追加MBSACLI檢測報告，可點選「新增壓縮檔」按鈕，透過上傳壓縮檔方式新增
– 須遵守上傳檔案注意事項

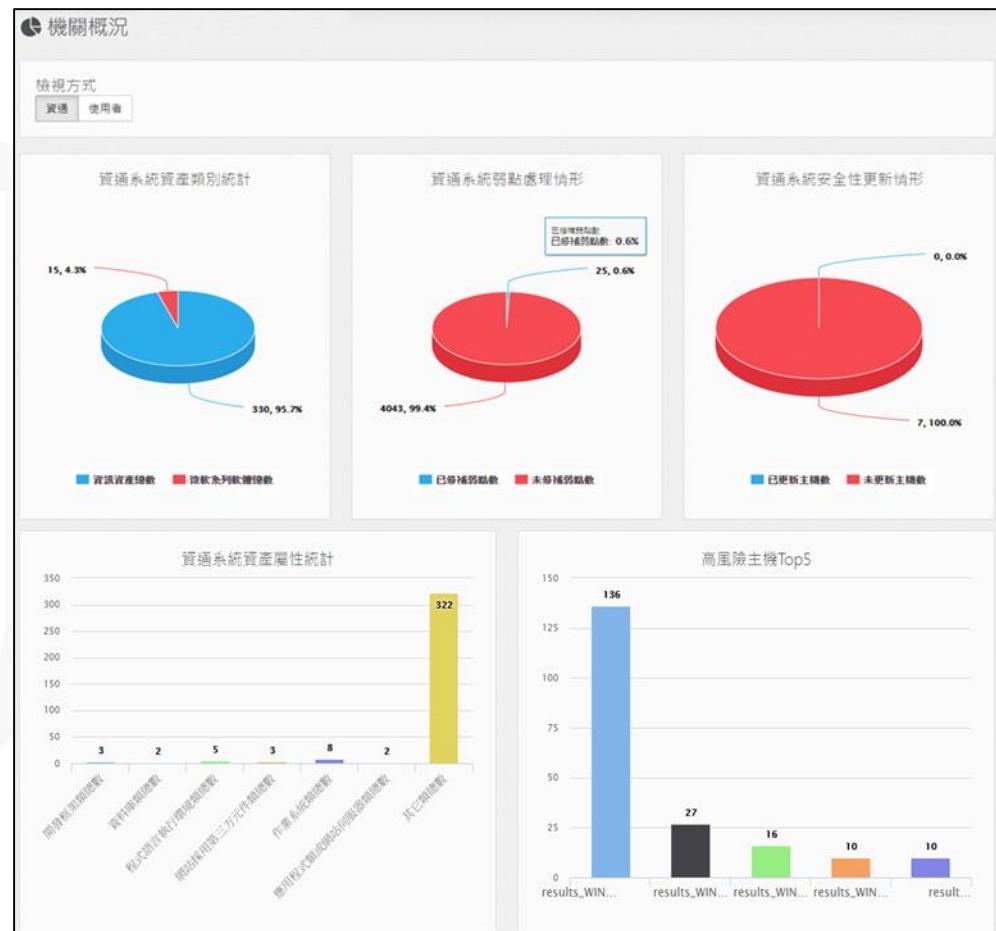
注意事項:

- 請將多份MBSACLI(MBSA的Command Line模式)檢測結果報告(XML檔)壓縮後上傳。
- 單次上傳壓縮檔大小限制為**20MB**以內，若檔案太大請分次上傳。
- 同一專案內，不可重複上傳同檔名之MBSACLI檢測結果報告。

功能介紹-機關概況

- 以統計圖表方式呈現機關資產與弱點概況，供機關定期檢視資訊資產狀態與弱點防護情形

- 資訊資產數量與類別
- CVE弱點處理情形
- Windows Update更新情形

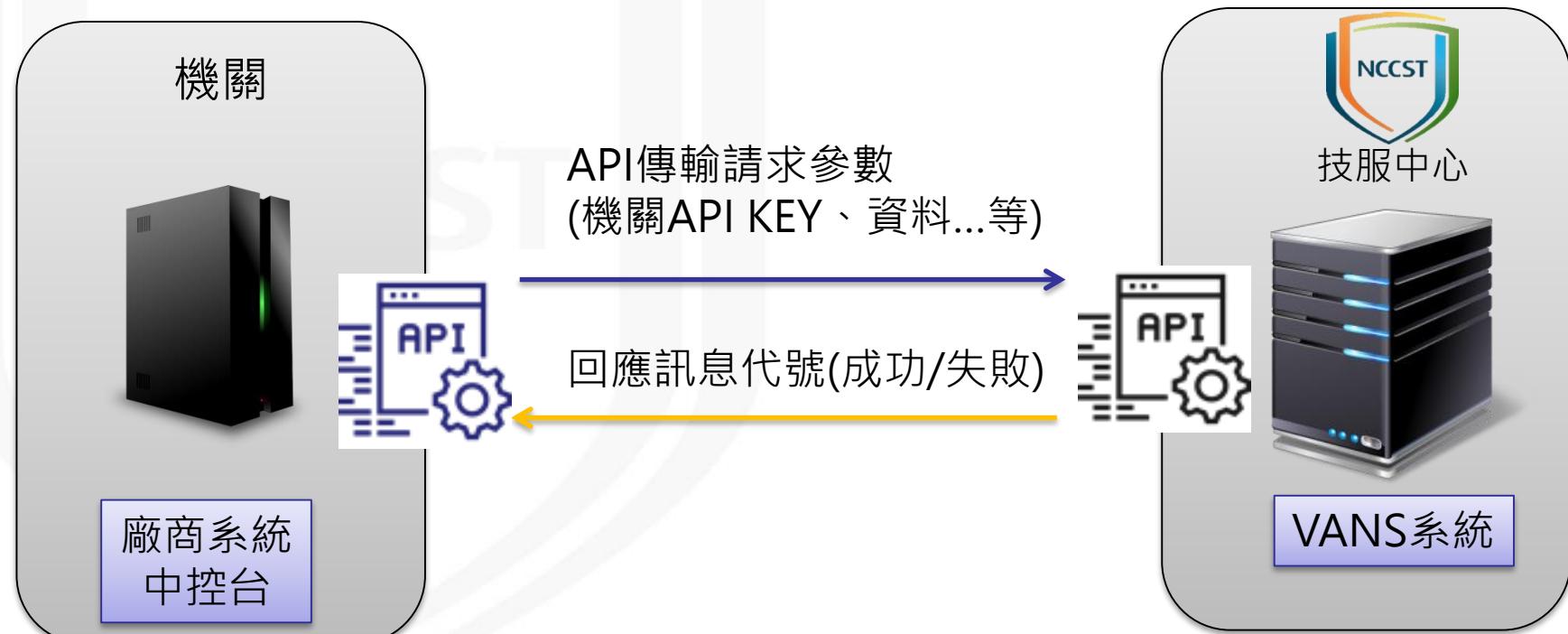


資產管理API功能說明(1/2)

API驗證項目



- IP位址：僅接受架設於機關之廠商中控台伺服器IP，方可執行上傳作業
- 機關API KEY(api_key)：機關可至VANS系統API功能頁面查看該機關專屬之API KEY



資產管理API功能說明(2/2)

- 各機關對應之API_key可於登入系統後，至「設定管理 > API設定」功能產生API_key



政府機關資安弱點通報機制

測試人員

機關概況

資訊資產管理

資產風險狀態

資訊查詢

設定管理

通知設定

一般帳號審核功能

一般帳號管理功能

解除登入鎖定功能

1. 資產管理API設定

2. 重新產生API key

設定管理 > 資產管理API設定

機關資產管理API key

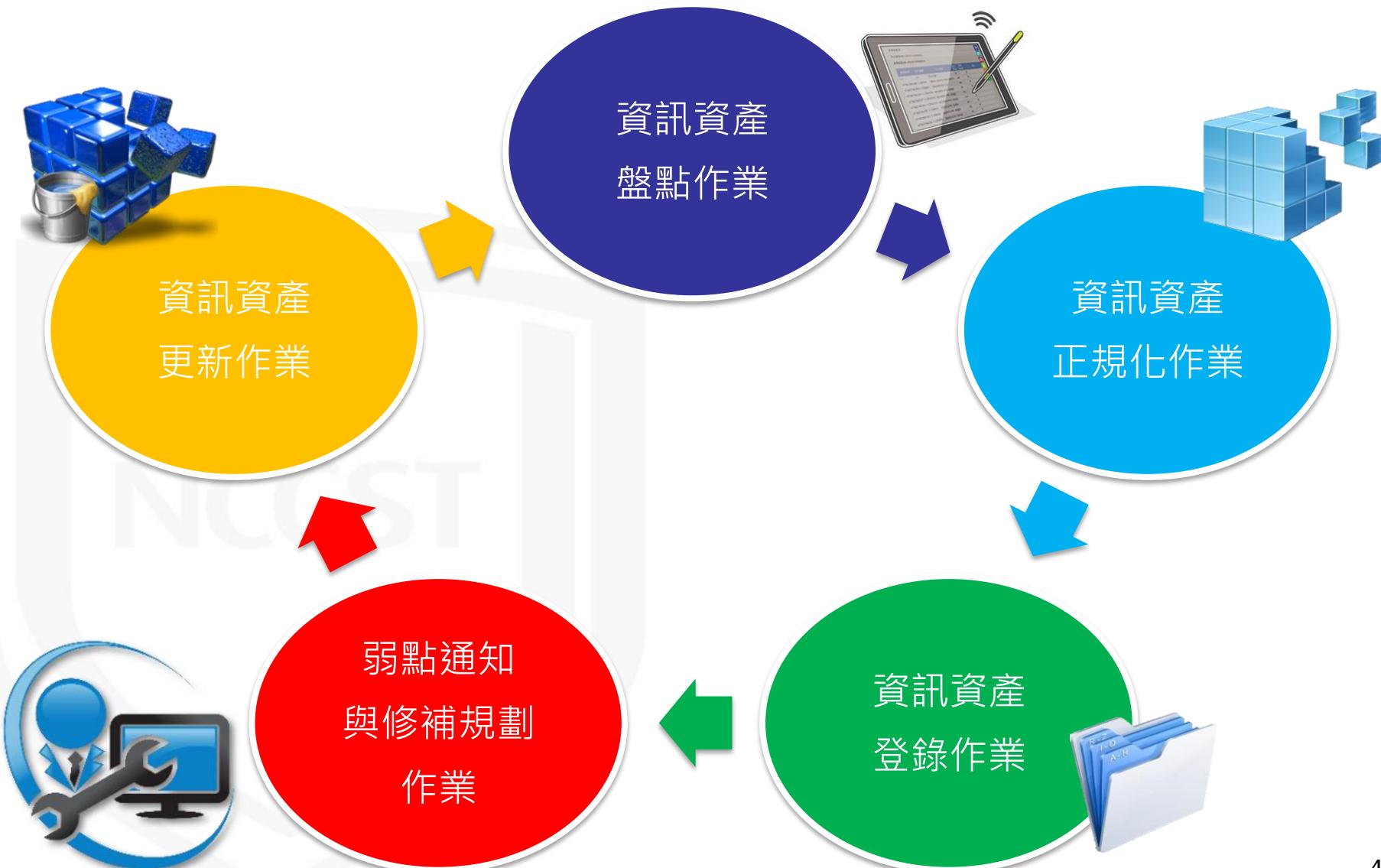
使用以下API key存取系統

尚未建立

大綱

- 前言
- 政府機關資安弱點通報機制
- 系統功能
- 實作建議
- 後續推動重點

系統作業流程



資訊資產盤點標的

- 蒐集範圍：資通系統與使用者電腦



Windows平台



應用程式

應用程式或網站伺服器

程式語言執行環境

網站採用第三方元件

開發框架

資料庫

- Adobe
- Apache



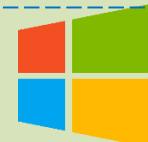
作業系統



Windows
Server 2012 R2



Windows Server 2016
Datacenter



Windows



Windows 8



Windows 10
Professional

- 軟體名稱
- 開發廠商名稱

- 版本資訊
- 軟體（安裝）數量

實作流程

透過可轉換CPE
格式之廠商工具
產出CPE格式報表



資訊系統

使用者電腦

搭配廠商工具盤點



透過系統指令或
工具盤點



透過CPE模組產
出CPE清單



彙整資料



比對以轉換為CPE格式

資訊資產CPE清單



登錄VANS系統

資產管理

軟體



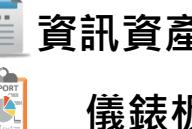
弱點管理



弱點通知



資訊綜整



資訊資產清單

儀錶板

透過AD派送批次檔
方式盤點軟、硬體資
產資訊，再以
PowerQuery擴充套
件彙整



VANS系統

實作案例(1/5)

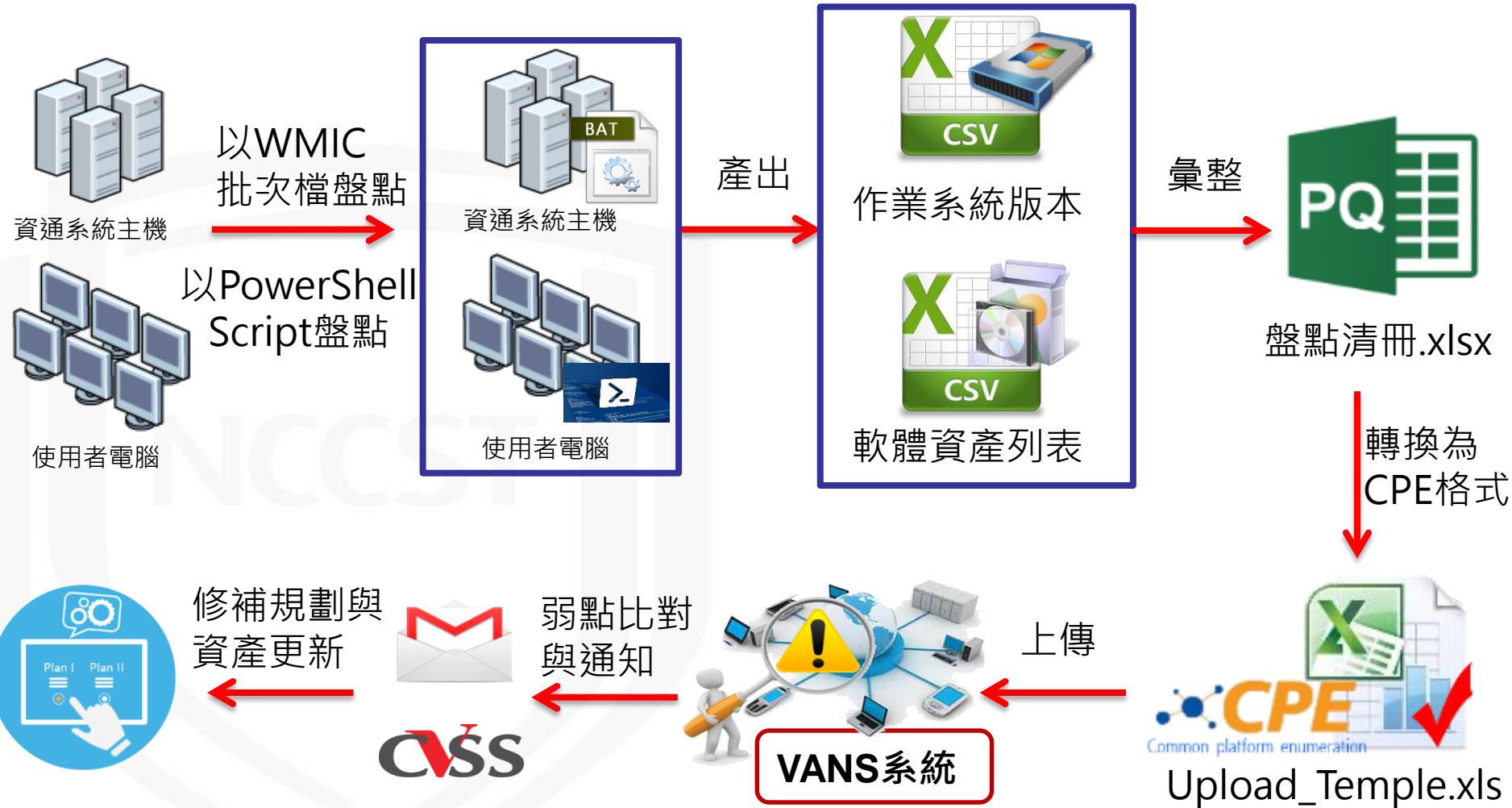
- 為強化政府機關資安防護措施，並因應「資通安全管理法」施行後之法遵義務，執行資安防護輔導服務，透過「輔導訓練課程」與「實地輔導」二項服務，共協助10個機關推動與落實各項資通安全防護作業
- 以下透過2個機關實地輔導案例，說明實作流程與結果

機關	導入範圍	實作方式
A機關	2台伺服器主機 8台使用者電腦	透過系統指令或工具盤點，並以完整資產CPE清單查找比對轉換為CPE格式清單
B機關	1台伺服器主機 11台使用者電腦	搭配廠商工具盤點，並以CPE模組產出CPE格式清單



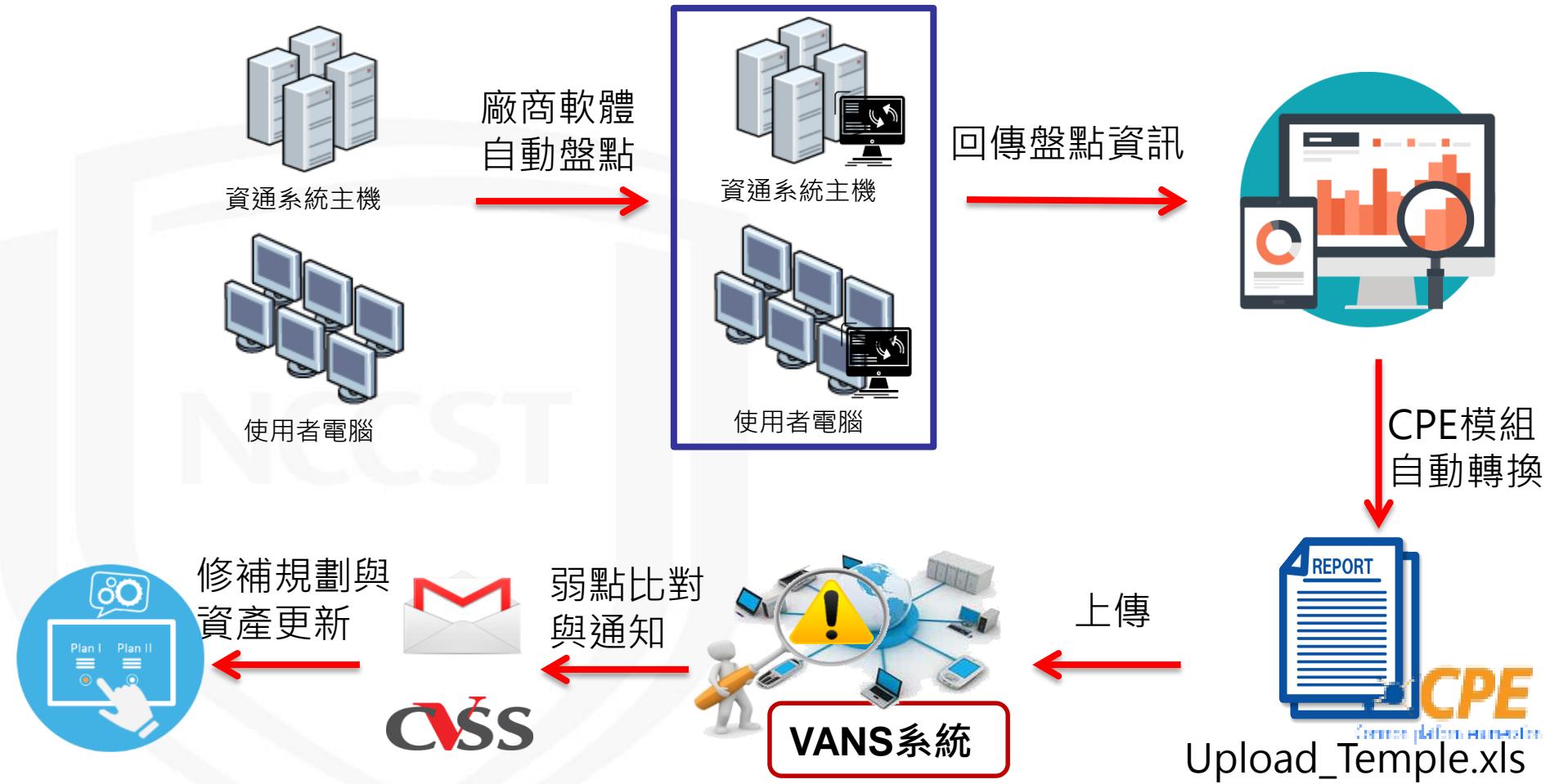
實作案例(2/5)

● A機關實作流程



實作案例(3/5)

● B機關實作流程



實作案例(4/5)

● A機關實作成果

機關	軟體資產數	微軟軟體CVE總數	非微軟軟體CVE總數
A機關	36	2,001	153

- 資通系統比對之弱點項目皆為微軟相關軟體，故透過MBSA檢查缺漏之安全性更新。於實地輔導期間已進行弱點修補規劃，並完成1個系統安全性更新修補作業
- 使用者電腦比對之弱點，於實地輔導後針對弱點比對結果進行修補規劃，並執行修補作業
 - 微軟軟體部分擬透過MBSA檢查缺漏之安全性更新
 - Python、Adobe Air、Adobe Acrobat Reader、VMware vSphere client、VMware Tools等非微軟軟體，將評估是否可透過升版或其他方式進行修補

實作案例(5/5)

● B機關實作成果

機關	軟體資產數	微軟軟體CVE總數	非微軟軟體CVE總數
B機關	26	3,908	402

– 資通系統與使用者電腦比對之弱點，於實地輔導後針對弱點比對結果進行修補規劃，並執行修補作業

- Windows、Office、SQL Server、.NET Framework等微軟相關資產，透過MBSA檢查缺漏之安全性更新
- Acrobat Reader DC、Firefox、VMware vSphere Client等非微軟軟體，將評估是否可透過升版或其他方式進行修補

大綱

- 前言
- 政府機關資通系統弱點通報機制
- 系統功能
- 實作建議
- 後續推動重點

後續推動重點

- 目前已有資安服務共契廠商提供CPE轉換功能，可降低所耗費之人力與時間
- VANS歷經試辦導入作業、推廣說明會、資安服務團等施行後，已依機關反應與建議精進強化，考量本機制已日趨成熟，後續將**評估納入應辦事項**，**每半年至少更新1次**資訊資產至VANS系統，期透過本機制進一步強化政府機關資訊資產之資安管理

服務申請流程





服務申請聯絡資訊

- 聯絡窗口：陳耕硯先生
- 聯絡電話：(02)6631-6458
- 聯絡信箱：julianchen@nccst.nat.gov.tw



報告完畢
敬請指教

NCCST

資安管理措施

- 因應系統存有機關的軟體資產資訊，在資料保護上有做以下保護措施
 - 管理面
 - 藉由資通系統分級作業、系統上線前測試、定期安全性檢查、關鍵業務審查作業、內部稽核及外部稽核等措施，確保本服務之資安品質
 - 技術面
 - 採SSDLC安全開發、身分驗證機制、登入鎖定功能、鎖定久未活動之一般帳號、帳號密碼相關防護機制、日誌紀錄及資料庫加密等措施，以降低資安風險