政府機關資安弱點通報系統操作說明

行政院國家資通安全會報技術服務中心

【普通】

大綱

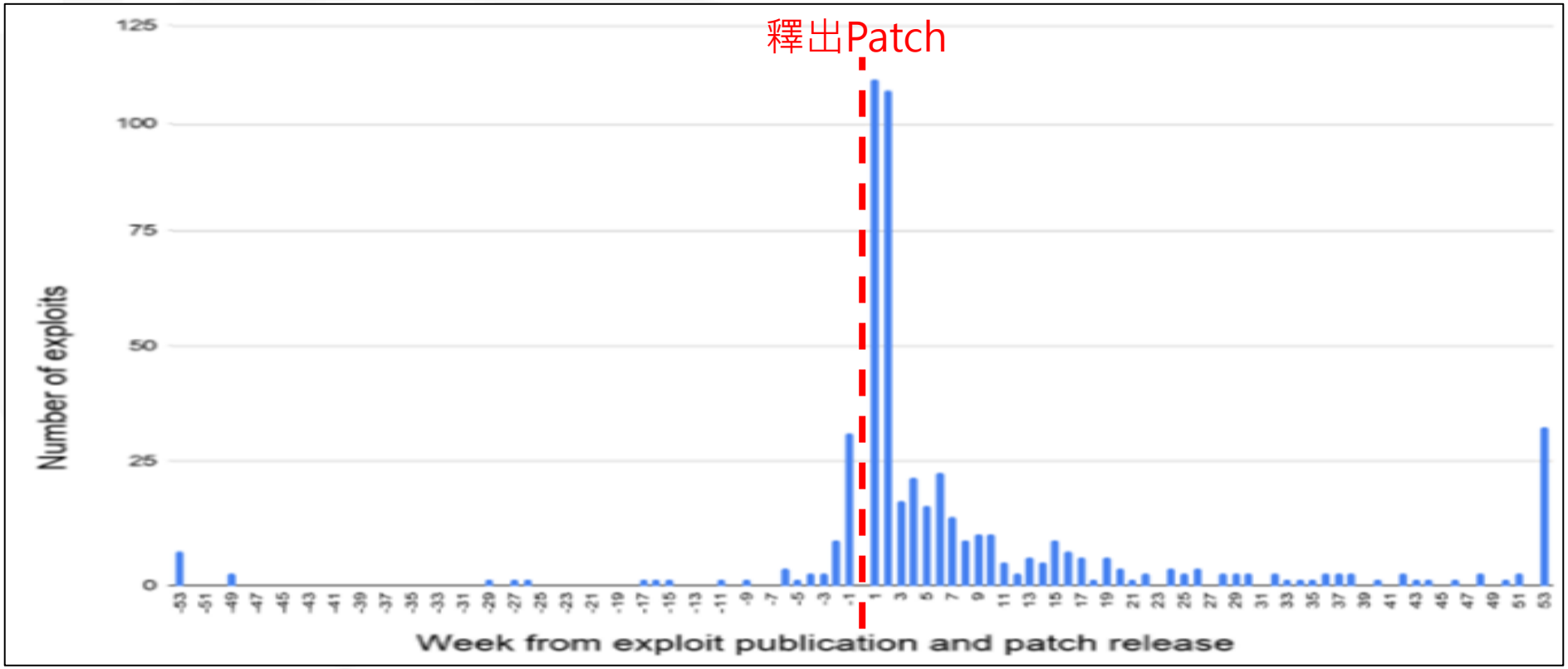
- 前言
- VANS系統介紹
- VANS系統操作說明
- 預期效益

大綱

- 前言
- VANS系統介紹
- VANS系統操作說明
- 預期效益

資安威脅與修補空窗期

- Unit 42威脅研究團隊抽樣檢視Exploit Database發現，2015至2020年期間所釋出之500個高風險弱點攻擊程式
  - 50%攻擊程式在廠商釋出修補程式後1個月內出現
  - 廠商釋出修補程式後，平均約37天出現攻擊程式



弱點應變關鍵

- 透過VANS系統之資產管理與弱點比對功能，可協助機關快速掌握弱點資訊與受影響範圍，以利及早進行弱點修補與追蹤

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
- VANS系統介紹
- VANS系統操作說明
- 預期效益

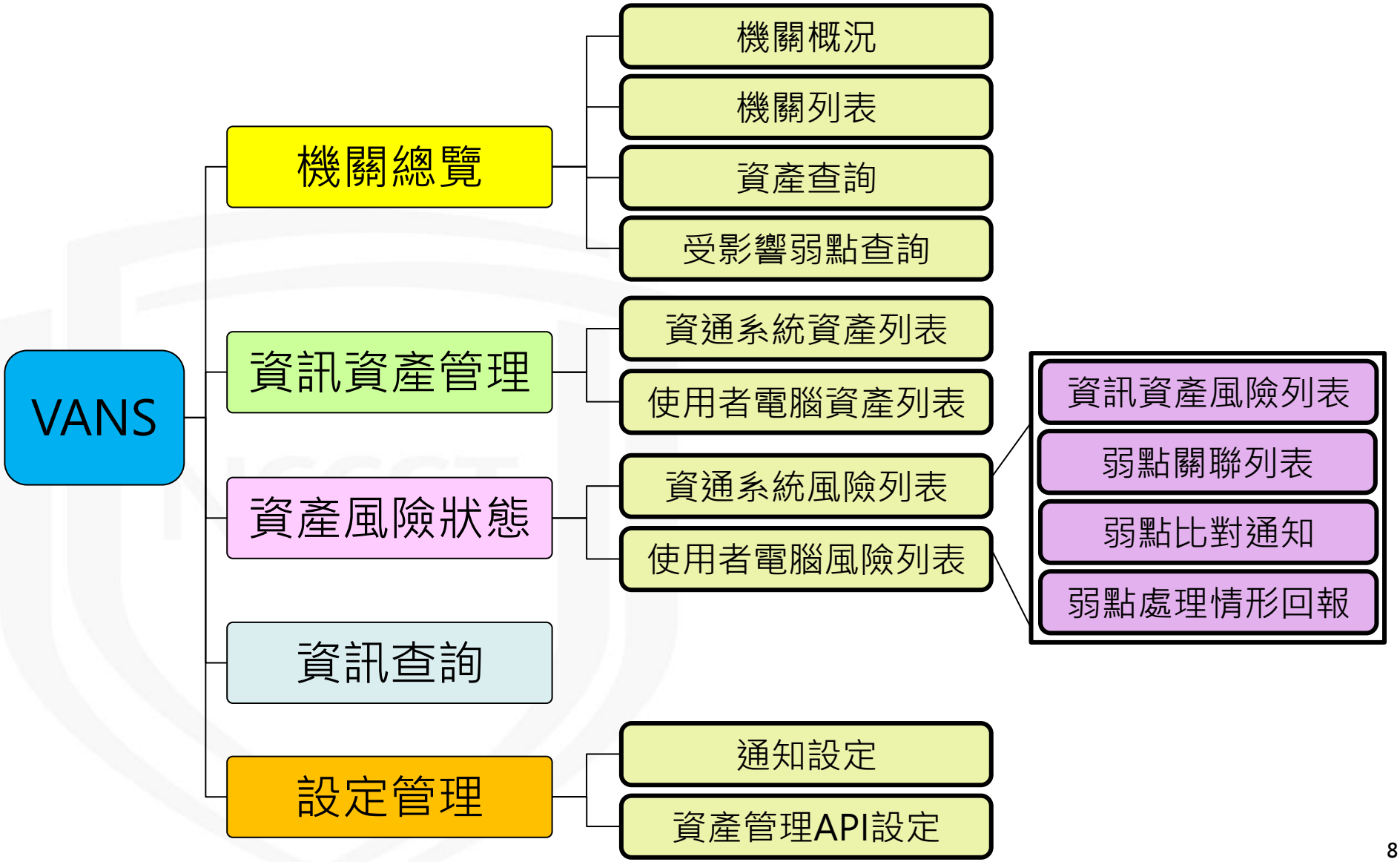
系統介紹

- VANS系統提供機關登錄資訊資產，藉由系統自動與NVD弱點資料庫比對，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

系統介面說明


系統名稱
登出
政府機關資安弱點通報系統
功能路徑
測試人員
機關總覽 > 機關概況
主畫面
首頁
機關總覽
機關概況
機關列表
資產查詢
受影響弱點查詢
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
檢視方式
資通系統
使用者電腦
資通系統資產類別統計
0, 0.0%
1, 100.0%
資訊資產總數
微軟系列軟體總數
資通系統弱點處理情形(CVE)
2.5%
27, 67.
已修補弱點數
未修補弱點數

系統功能總覽


VANS
機關總覽
機關概況
機關列表
資產查詢
受影響弱點查詢
資訊資產管理
資通系統資產列表
使用者電腦資產列表
資產風險狀態
資通系統風險列表
使用者電腦風險列表
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
資訊查詢
設定管理
通知設定
資產管理API設定

帳號權限

- 機關登入VANS系統分為下列兩種帳號權限

機關管理者帳號

- ✓ 檢視機關總覽
- ✓ 資訊資產與已安裝KBID管理
- ✓ 弱點管理
- ✓ 資訊查詢
- ✓ 檢視**機關各帳號**資產異動紀錄
- ✓ **重新產生**API Key

一般權限帳號

- ✓ 檢視機關總覽
- ✓ 資訊資產與已安裝KBID管理
- ✓ 弱點管理
- ✓ 資訊查詢
- ✓ 檢視**自身**帳號資產異動紀錄
- ✓ **檢視**API Key

系統安全管理措施

- 管理面
  - 藉由資通系統分級作業、系統上線前測試、定期安全性檢測、關鍵業務審查作業、內部稽核及外部稽核等措施，確保VANS系統之安全品質
- 技術面
  - 採行SSDLC安全開發、身分驗證機制、登入鎖定功能、鎖定久未活動閒置帳號、帳號密碼相關防護機制、日誌紀錄及資料庫加密等措施，防範資安風險

大綱

- 前言
- VANS系統介紹
- VANS系統操作說明
- 預期效益

導入作業流程

資訊資產與
已安裝KBID
更新作業

資訊資產與
已安裝KBID
盤點作業

資訊資產與
已安裝KBID
正規化作業

資訊資產與
已安裝KBID
登錄作業

弱點通知
與修補作業

導入作業流程-1

資訊資產與
已安裝KBID
盤點作業

資訊資產與
已安裝KBID
正規化作業

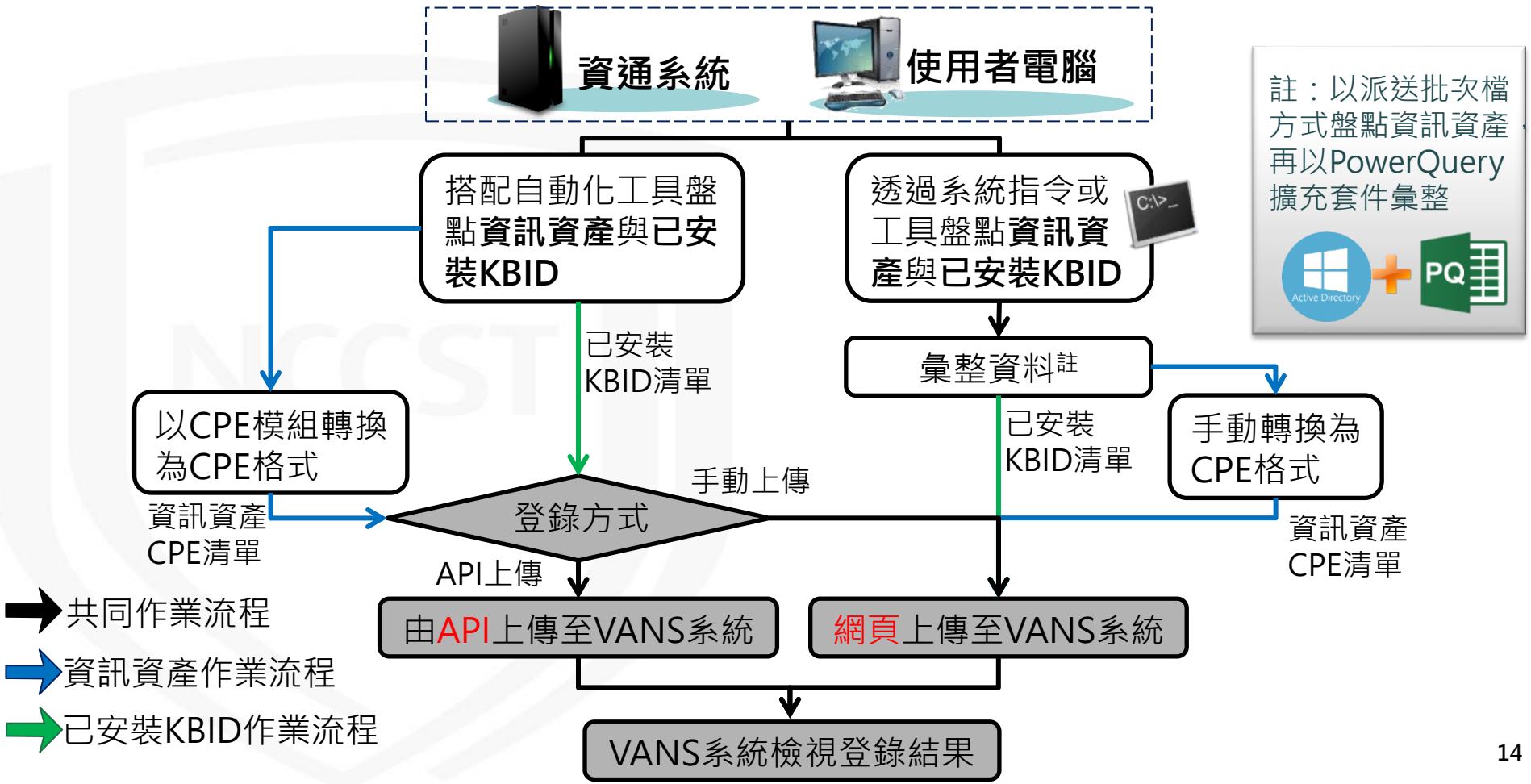
資訊資產與
已安裝KBID
登錄作業

弱點通知
與修補作業

資訊資產與
已安裝KBID
更新作業

資訊資產與已安裝KBID盤點與正規化作業

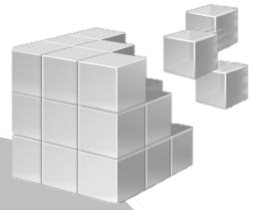
- 定期透過自動化工具或系統指令進行資訊資產與已安裝KBID之盤點與正規化，以利後續可登錄至VANS系統



導入作業流程-2

資訊資產與
已安裝KBID
更新作業

資訊資產與
已安裝KBID
盤點作業



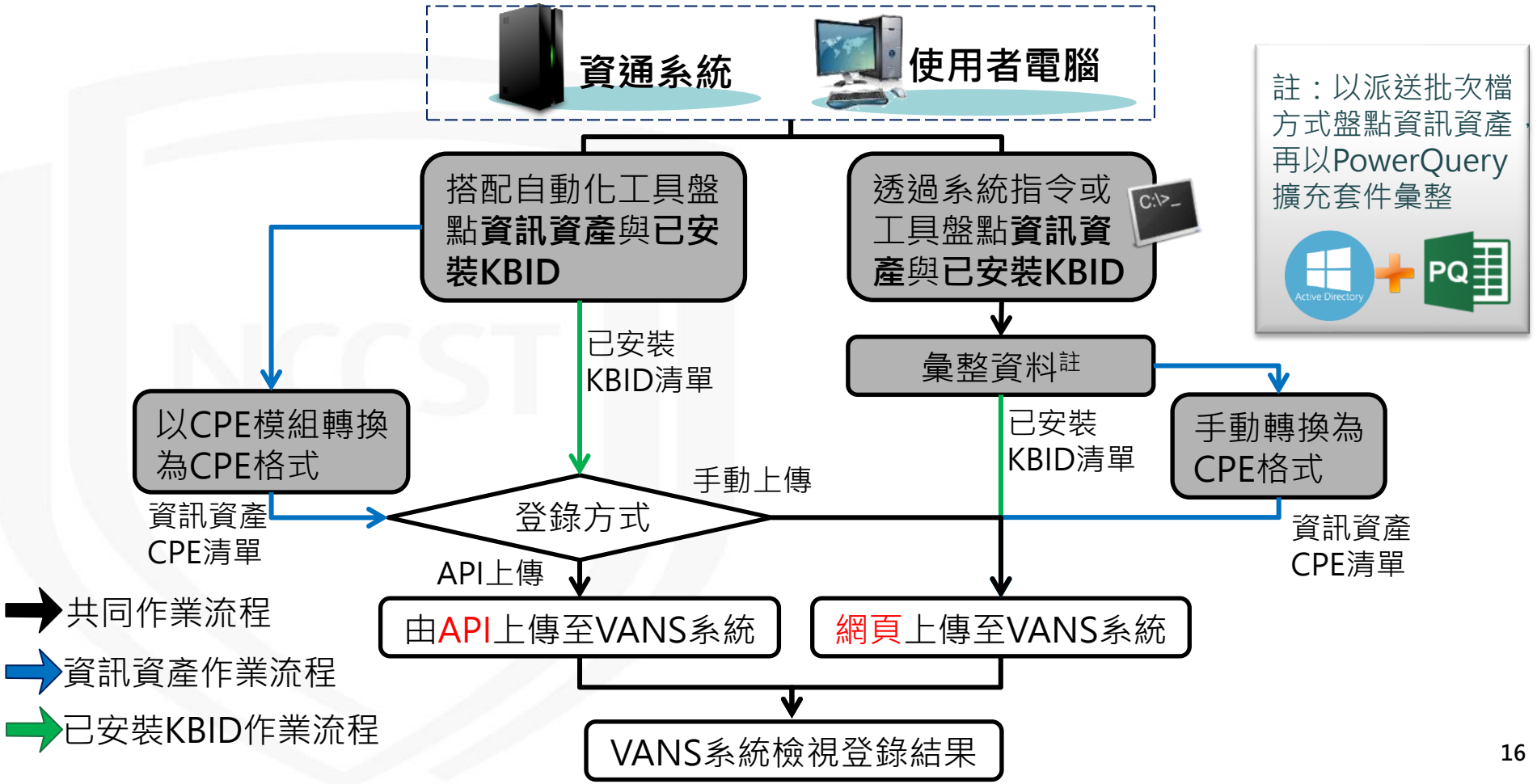
資訊資產與
已安裝KBID
正規化作業

資訊資產與
已安裝KBID
登錄作業

弱點通知
與修補作業

資訊資產與已安裝KBID登錄作業

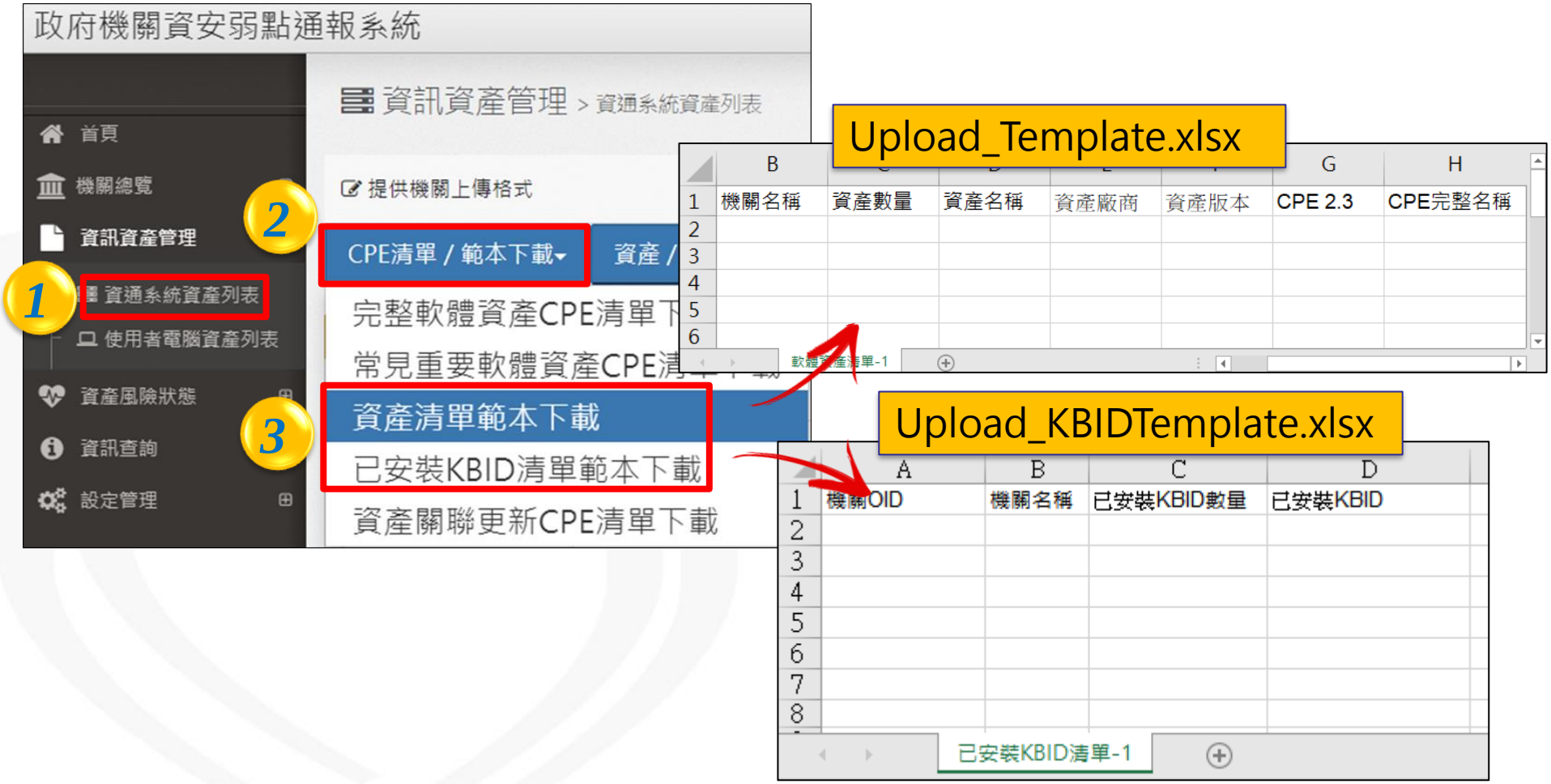
- 產出「資訊資產CPE清單」與「已安裝KBID清單」後，可選擇透過網頁或API方式進行登錄



註：以派送批次檔方式盤點資訊資產，再以PowerQuery擴充套件彙整

以網頁方式登錄(1/5)

- 下載資產清單與已安裝KBID清單之填寫格式



以網頁方式登錄(2/5)

- 蒐集各電腦資訊與已安裝更新編號(KBID)資訊
  - 資產清單列出資產名稱、資產廠商、資產版本及數量
  - 已安裝KBID清單列出已安裝更新編號(KBID)與數量

Apache Tomcat	KB4516115
Java 8 Update	KB4521863
...	KB4528759
	KB4561600
	...

Microsoft Windows Server 2019	KB4516115
exchange_ server	KB4521863
...	KB4528759
	KB4561600
	...

Exchange_ server	KB4516115
...	KB4561600
	...

Upload_Template.xlsx

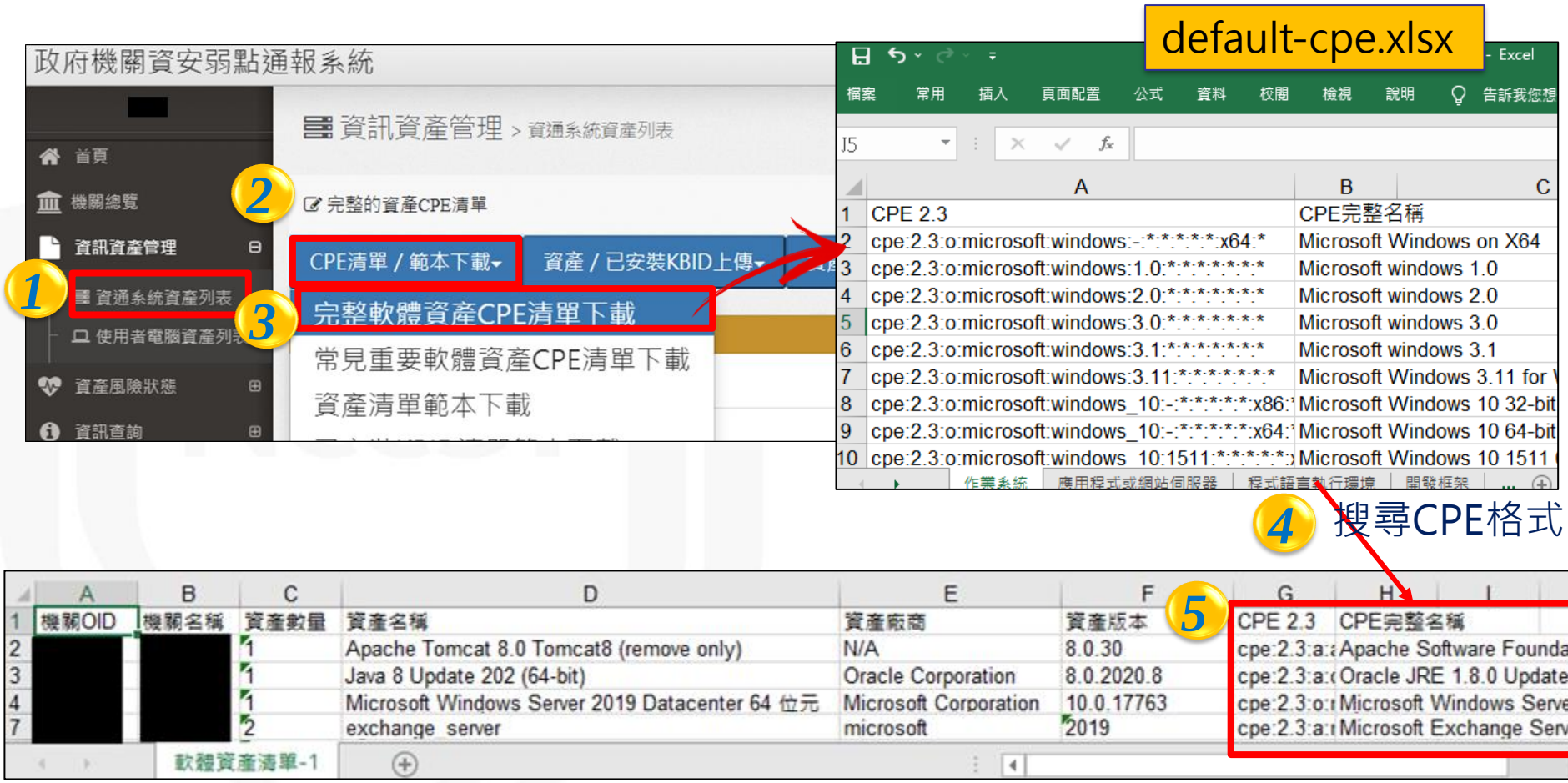
C	D	E	F
資產數量	資產名稱	資產廠商	資產版本
1	Apache Tomcat 8.0 Tomcat8 (remove only)	N/A	8.0.30
1	Java 8 Update 202 (64-bit)	Oracle Corporation	8.0.2020.8
1	Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft Corporation	10.0.17763
2	exchange_server	microsoft	2019

Upload_KBIDTemplate.xlsx

	A	B	C	D
1	機關OID	機關名稱	已安裝KBID數量	已安裝KBID
2	[redacted]	[redacted]	3	KB4516115
3			2	KB4521863
4			2	KB4528759
5			3	KB4561600

以網頁方式登錄(3/5)

- 下載「完整軟體資產CPE清單」並透過搜尋方式，完成「Upload_Template」中CPE格式欄位



以網頁方式登錄(4/5)

- 將彙整完成之資訊資產CPE清單與已安裝KBID清單透過網頁上傳

以網頁方式登錄(5/5)

- 上傳後，系統解析完成時，將寄送解析完成通知信

VANS <vans@nccst.nat.gov.tw>
[VANS]資通系統資訊資產清單解析完成
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系統」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 系統上傳之資訊資產清單已解析完成，請至 VANS 系統檢視資訊資產清單登錄結果。

謝謝。

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

如有任何疑問，聯絡資訊如下：
行政院國家資通安全會報技術服務中心(技服中心)
服務電話：(02)6631-6458
服務信箱：VansService@nccst.nat.gov.tw

VANS <vans@nccst.nat.gov.tw>
[VANS]資通系統已安裝KBID清單解析完成

敬啟者 您好

此為「政府機關資安弱點通報系統」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 系統上傳之已安裝 KBID 清單已解析完成，請至 VANS 系統檢視已安裝 KBID 清單登錄結果。

謝謝。

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

如有任何疑問，聯絡資訊如下：
行政院國家資通安全會報技術服務中心(技服中心)
服務電話：(02)6631-6458
服務信箱：VansService@nccst.nat.gov.tw

以API方式登錄(1/3)

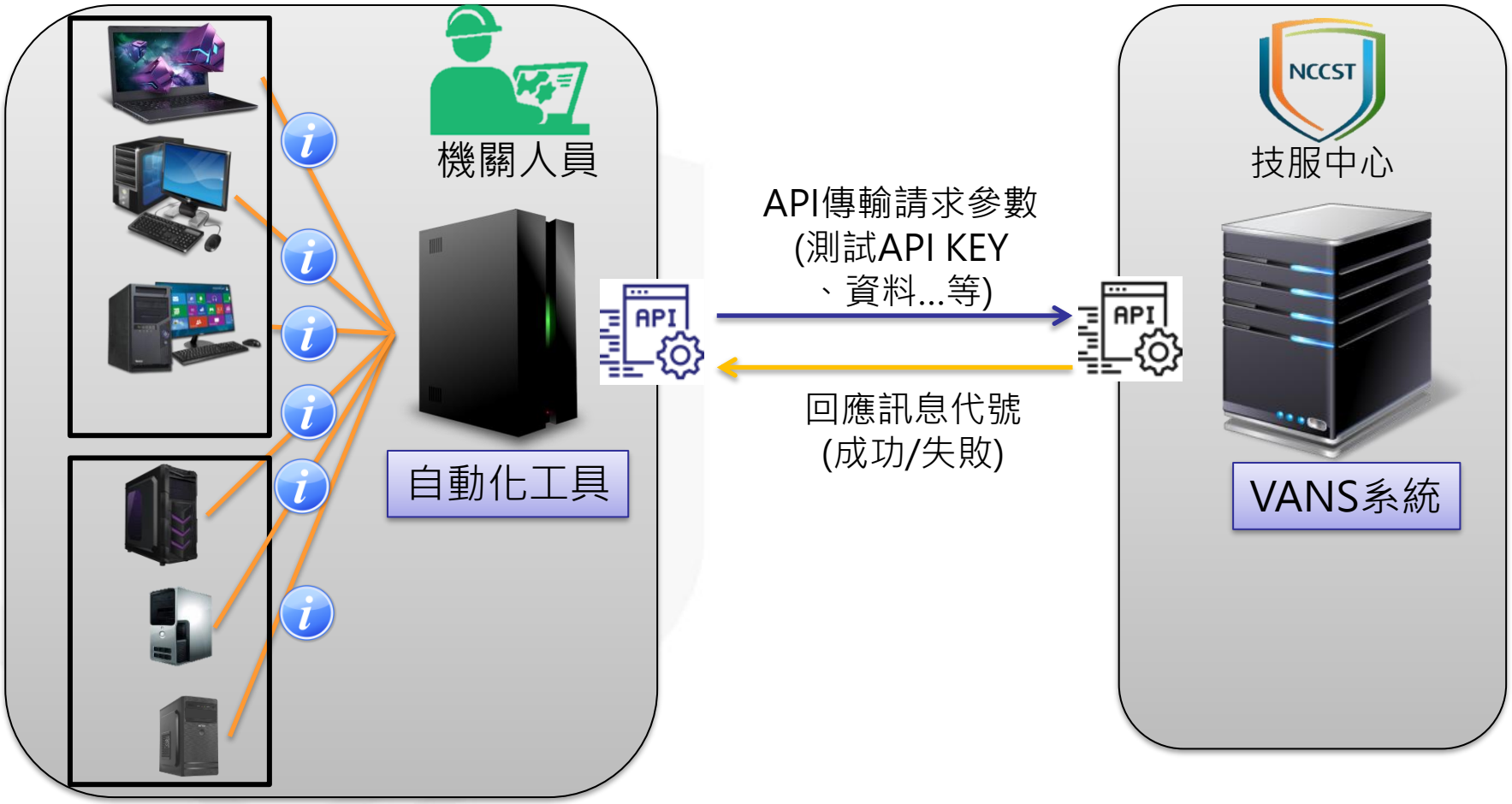
- 於VANS專區下載並填寫「政府機關資安弱點通報系統(VANS系統)API介接申請(異動)單」，針對欲與VANS系統介接之IP提出申請

以API方式登錄(2/3)

- 於VANS系統「資產管理API設定」查看機關專屬之API KEY，若尚未取得API key，可由機關管理者帳號點選「重新產生API key」
- VANS系統將於傳輸時確認該API KEY是否具備標的機關資訊資產或已安裝KBID上傳之權限

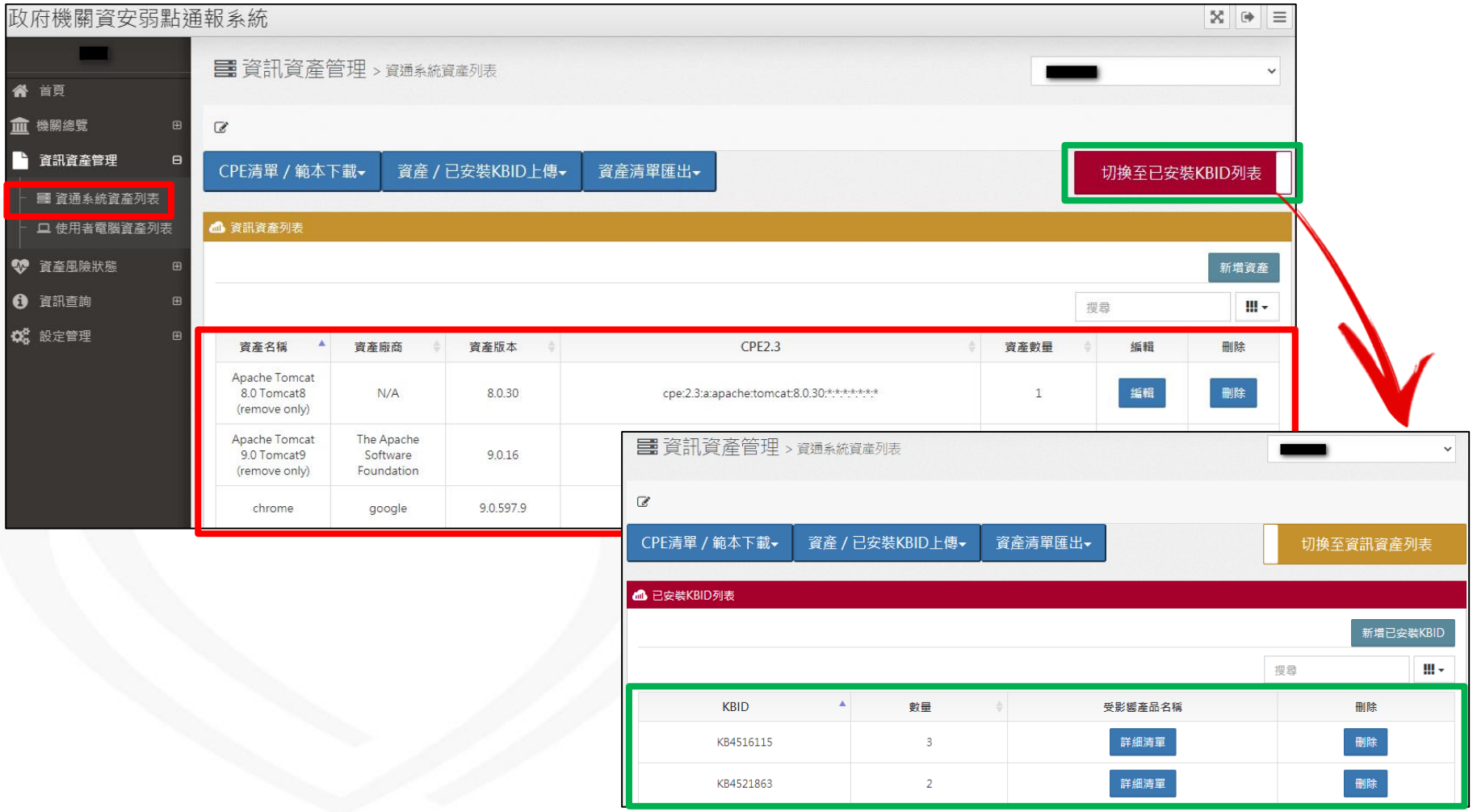
以API方式登錄(3/3)

- 將資訊資產與已安裝KBID以工具盤點後，透過API傳輸即可登錄至VANS系統



檢視登錄結果

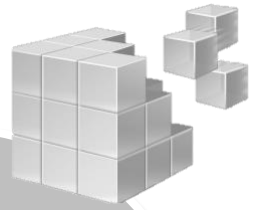
- 可於資訊資產管理功能查看登錄至VANS系統之資訊資產與已安裝KBID



導入作業流程-3

資訊資產與
已安裝KBID
更新作業

資訊資產與
已安裝KBID
盤點作業



資訊資產與
已安裝KBID
正規化作業

資訊資產與
已安裝KBID
登錄作業

弱點通知
與修補作業

弱點比對與通知

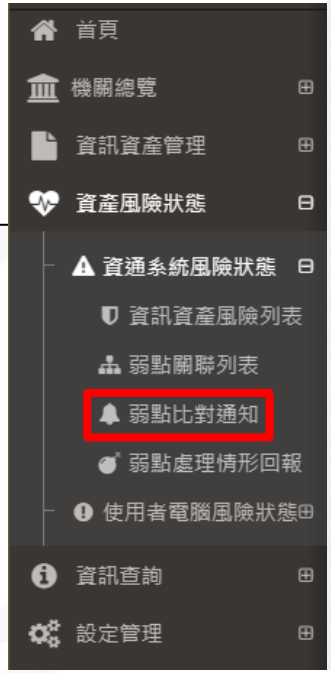
- VANS系統自動化比對機關登錄之資訊資產，符合下列條件時啟動弱點比對
  - 每日與NVD弱點資料更新後，比對整個VANS系統登錄之資訊資產
  - 個別機關資訊資產異動後，比對該機關於VANS系統登錄之資訊資產，惟避免頻繁異動造成整體比對作業延遲，個別機關最短比對間隔設定為2小時
- 弱點自動比對完成後，針對開啟弱點通知功能之機關，VANS系統將依機關設置之CVSS分數門檻發送弱點通知
  - 發送通知信予接收通知Email
  - 於VANS系統上顯示弱點比對通知
- 同一項資產之同一個弱點只會於首次比對到時進行1次通知，不會重複通知

弱點通知設定(1/2)

- 可於通知設定調整弱點通知分數門檻與接收Email

弱點通知設定(2/2)

- 機關收到弱點通知信後，請至VANS系統確認。弱點通知內容包含通知時間、資產數量及弱點數量等

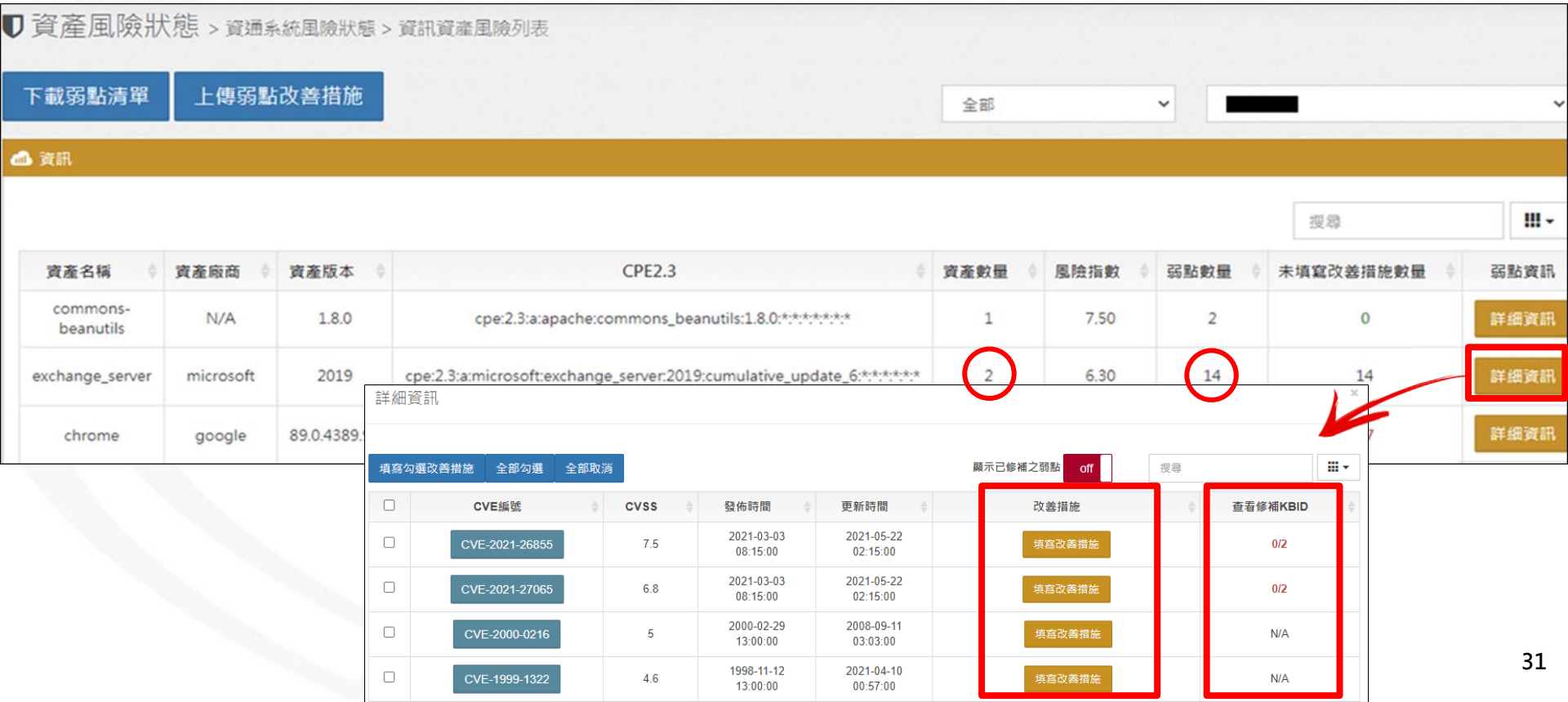


弱點確認與修補

- 透過資訊資產風險列表，檢視各資訊資產存在之弱點與弱點處理情形
  - 案例1：微軟類弱點修補方式(Exchange Server 2019)
  - 案例2：非微軟類弱點修補方式(Google Chrome 89.0.4389.90)

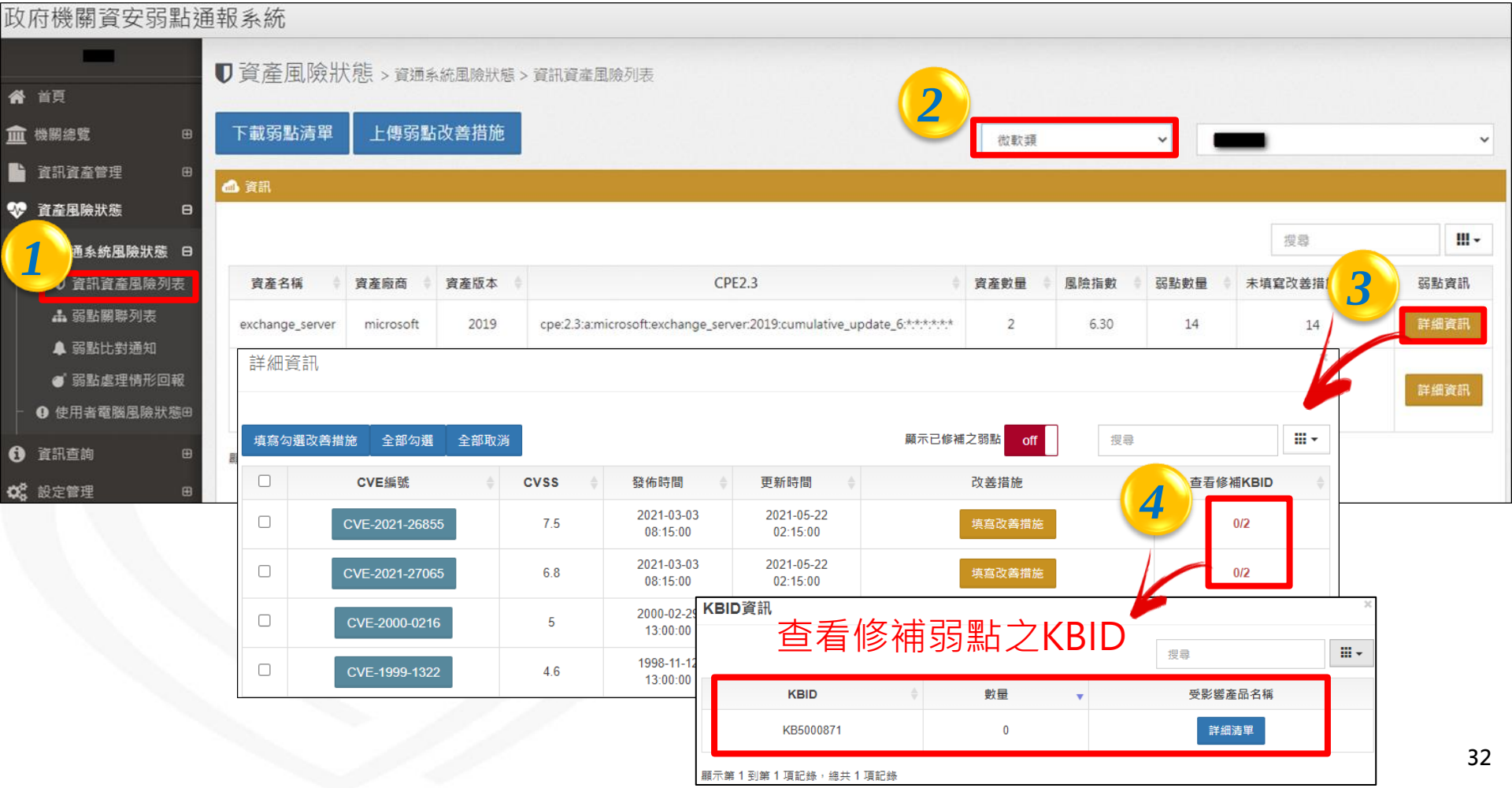
案例1：弱點處理情形

- 透過資訊資產風險列表，可得知目前全機關資通系統共安裝2套Exchange Server 2019，尚有14個弱點未處理
- 微軟類資產修補方式分為下列2種：
  - 透過KBID修補之弱點，於查看修補KBID欄位檢視弱點是否修補
  - 非透過KBID修補之弱點，於改善措施欄位進行修補規劃



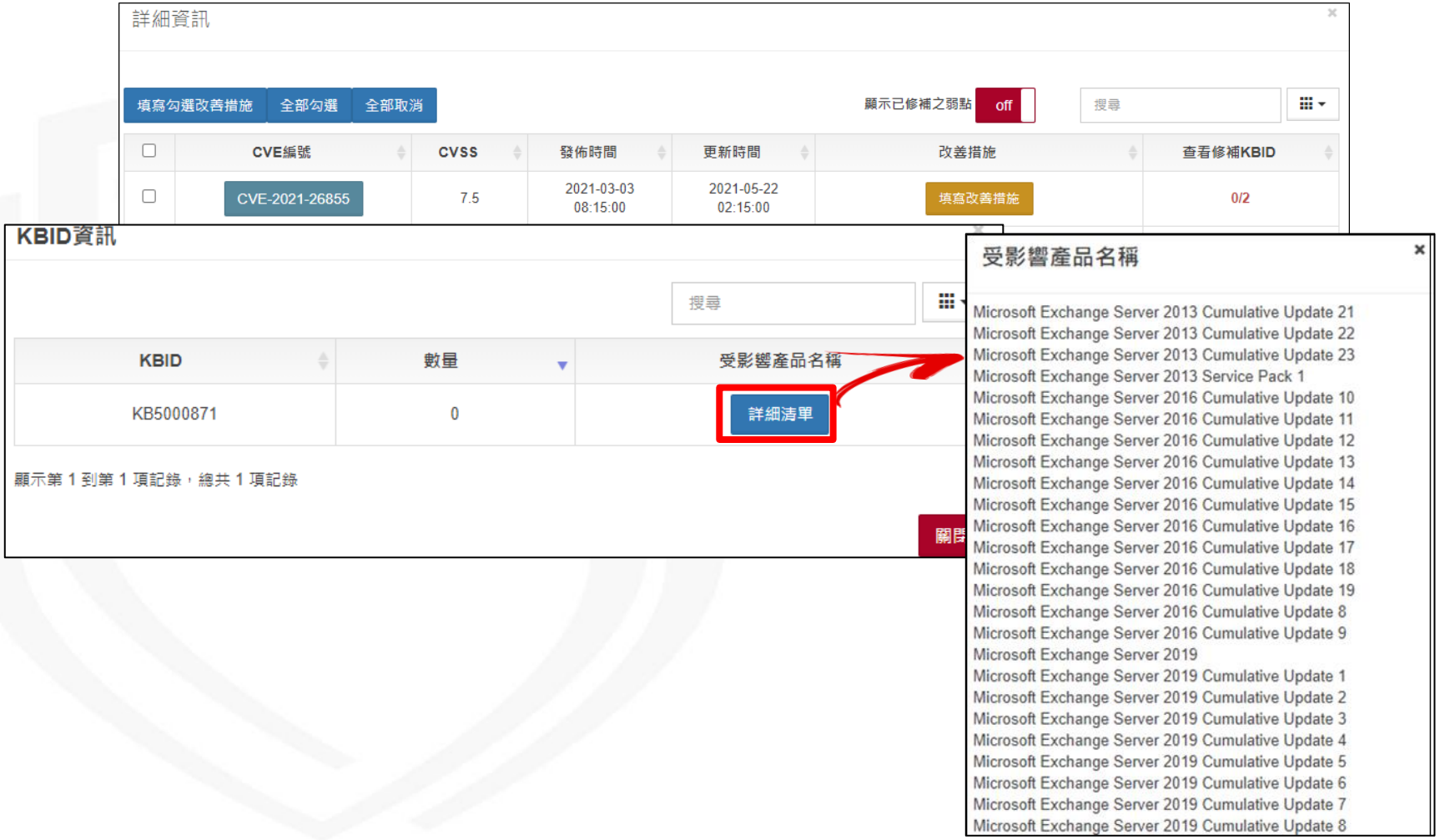
案例1：確認弱點(1/2)

- 針對透過安全性更新修補之弱點，可點選查看修補KBID，檢視修補此弱點應安裝之KBID



案例1：確認弱點(2/2)

- 透過受影響產品名稱，檢視該KBID可修補之產品
- 更新前，建議進行評估與測試

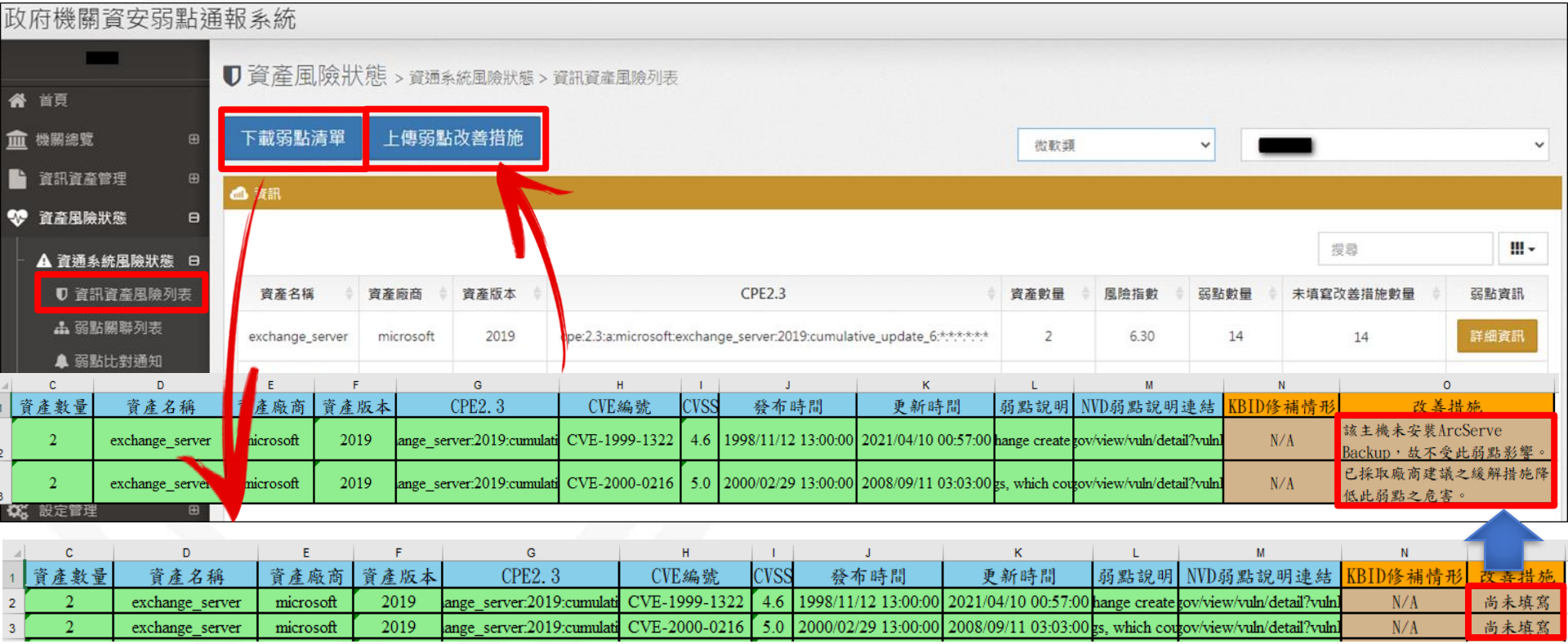


案例1：弱點修補(1/2)

- 針對非透過安全性更新修補之弱點，請於改善措施填寫處理方式

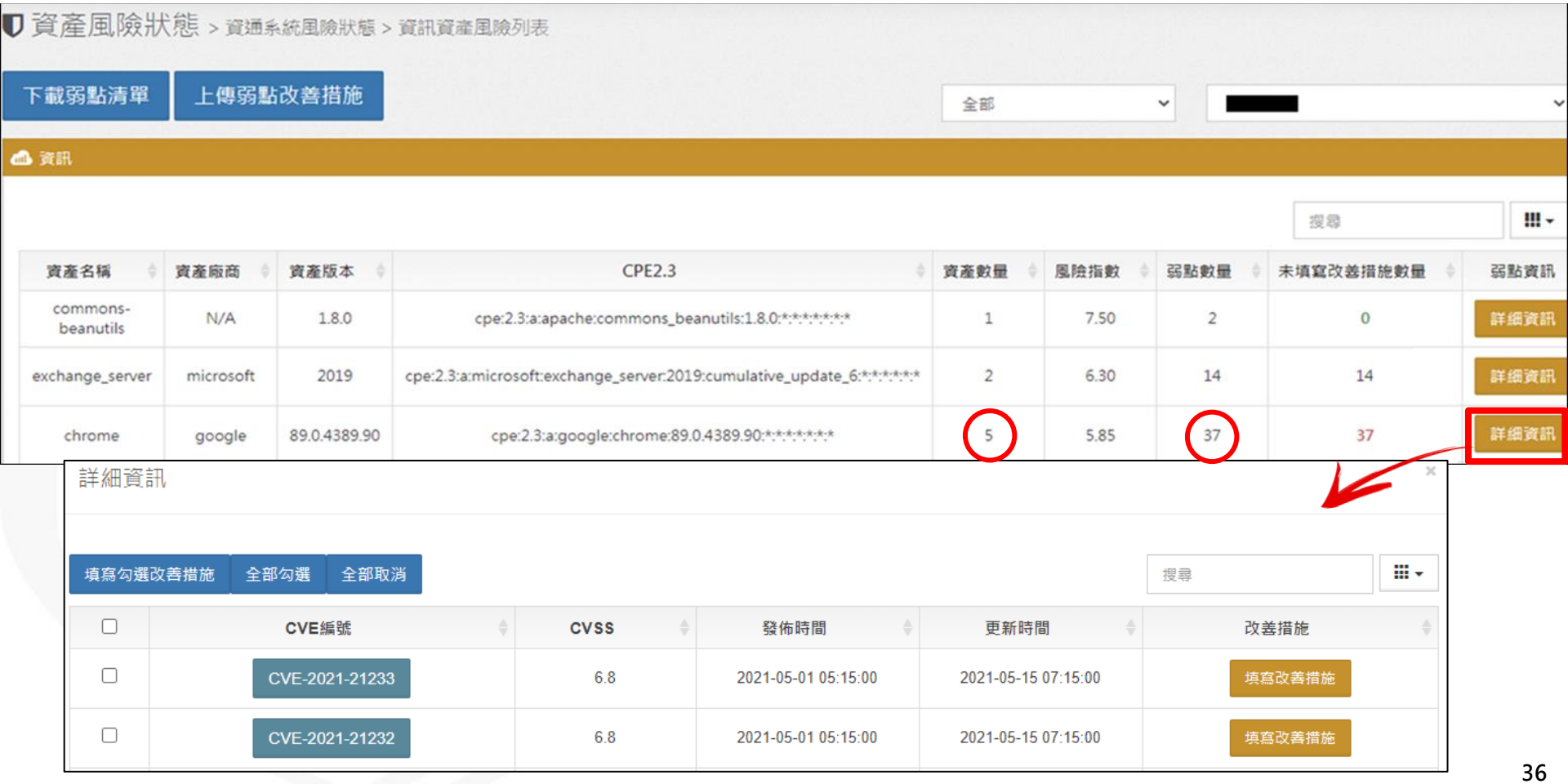
案例1：弱點修補(2/2)

- 可下載弱點清單提供予資通系統/使用者電腦負責人，完成修補評估與處理後，上傳弱點清單以登錄改善措施至VANS系統



案例2：弱點處理情形

- 透過資訊資產風險列表，可得知目前全機關資通系統共安裝5套Google Chrome 89.0.4389.90版本，尚有37個弱點未處理



案例2：確認弱點(1/3)

- 針對各個弱點，可點選CVE編號按鈕(如CVE-2021-21233)，檢視弱點描述與相關連結

案例2：確認弱點(2/3)

- 參閱NVD官網建議弱點修補方式

References to Advisories, Solutions, and Tools

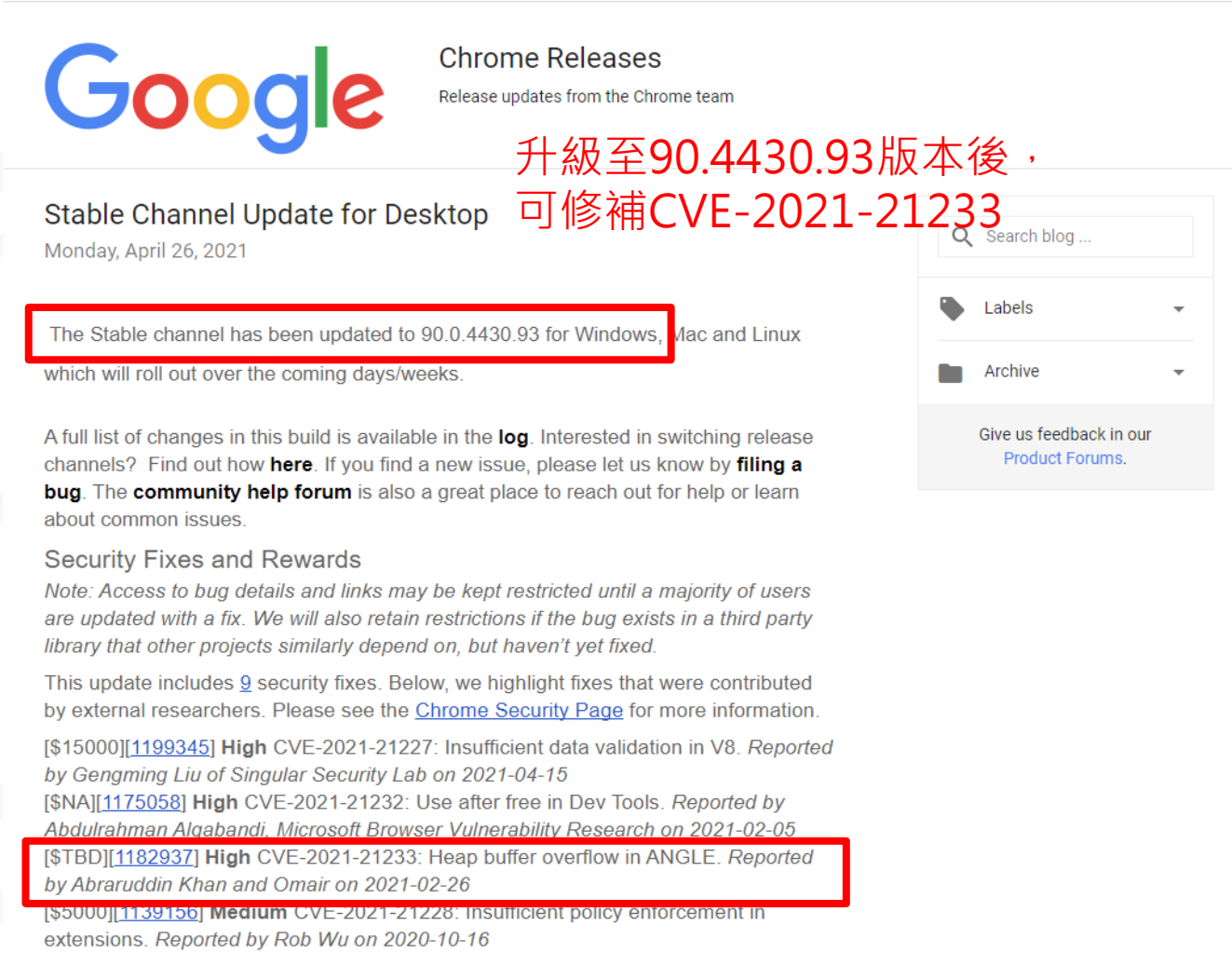
By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_26.html	Release Notes Vendor Advisory
https://crbug.com/1182937	Permissions Required Vendor Advisory
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/EAJ42L4JFPBJATCZ7MOZQTUDGV4OEHHG/	Mailing List Third Party Advisory
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/U3GZ42MYPGD35V652ZPVPYYS7A7LVXVY/	Mailing List Third Party Advisory
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/VUZBGKGVZADNA3I24NVG7HAYYUTOSN5A/	Mailing List Third Party Advisory
https://security.gentoo.org/glsa/202104-08	Third Party Advisory
https://www.debian.org/security/2021/dsa-4911	Third Party Advisory

原廠說明連結

案例2：確認弱點(3/3)

- 查閱原廠或資安廠商建議弱點修補方式



Google

Chrome Releases

Release updates from the Chrome team

升級至90.4430.93版本後，
可修補CVE-2021-21233

Stable Channel Update for Desktop

Monday, April 26, 2021

The Stable channel has been updated to 90.0.4430.93 for Windows, Mac and Linux which will roll out over the coming days/weeks.

A full list of changes in this build is available in the **log**. Interested in switching release channels? Find out how **here**. If you find a new issue, please let us know by **filing a bug**. The **community help forum** is also a great place to reach out for help or learn about common issues.

Security Fixes and Rewards

Note: Access to bug details and links may be kept restricted until a majority of users are updated with a fix. We will also retain restrictions if the bug exists in a third party library that other projects similarly depend on, but haven't yet fixed.

This update includes 9 security fixes. Below, we highlight fixes that were contributed by external researchers. Please see the Chrome Security Page for more information.

[$15000][1199345] **High** CVE-2021-21227: Insufficient data validation in V8. *Reported by Gengming Liu of Singular Security Lab on 2021-04-15*

[$NA][1175058] **High** CVE-2021-21232: Use after free in Dev Tools. *Reported by Abdulrahman Alqabandi, Microsoft Browser Vulnerability Research on 2021-02-05*

[$TBD][1182937] **High** CVE-2021-21233: Heap buffer overflow in ANGLE. *Reported by Abraruddin Khan and Omair on 2021-02-26*

[$5000][1139156] **Medium** CVE-2021-21228: Insufficient policy enforcement in extensions. *Reported by Rob Wu on 2020-10-16*

Search blog ...

Labels

Archive

Give us feedback in our Product Forums.

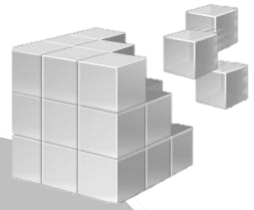
案例2：弱點修補

- 依據機關ISMS政策所訂定之弱點修復基準與修復時程進行修補
- 針對無法立即修補或須接受風險之弱點，可進行評估與測試，並於VANS系統填寫改善措施

導入作業流程-4

資訊資產與
已安裝KBID
更新作業

資訊資產與
已安裝KBID
盤點作業



資訊資產與
已安裝KBID
正規化作業

資訊資產與
已安裝KBID
登錄作業

弱點通知
與修補作業

資訊資產更新(1/2)

- 更新Google Chrome至90.0.4430.93版本，並於VANS系統更新資訊資產

資訊資產更新(2/2)

- 因Google Chrome 90.0.4430.93版本目前未有CVE弱點，故重新比對弱點後，資訊資產風險列表已無Google Chrome相關弱點

已安裝KBID更新(1/2)

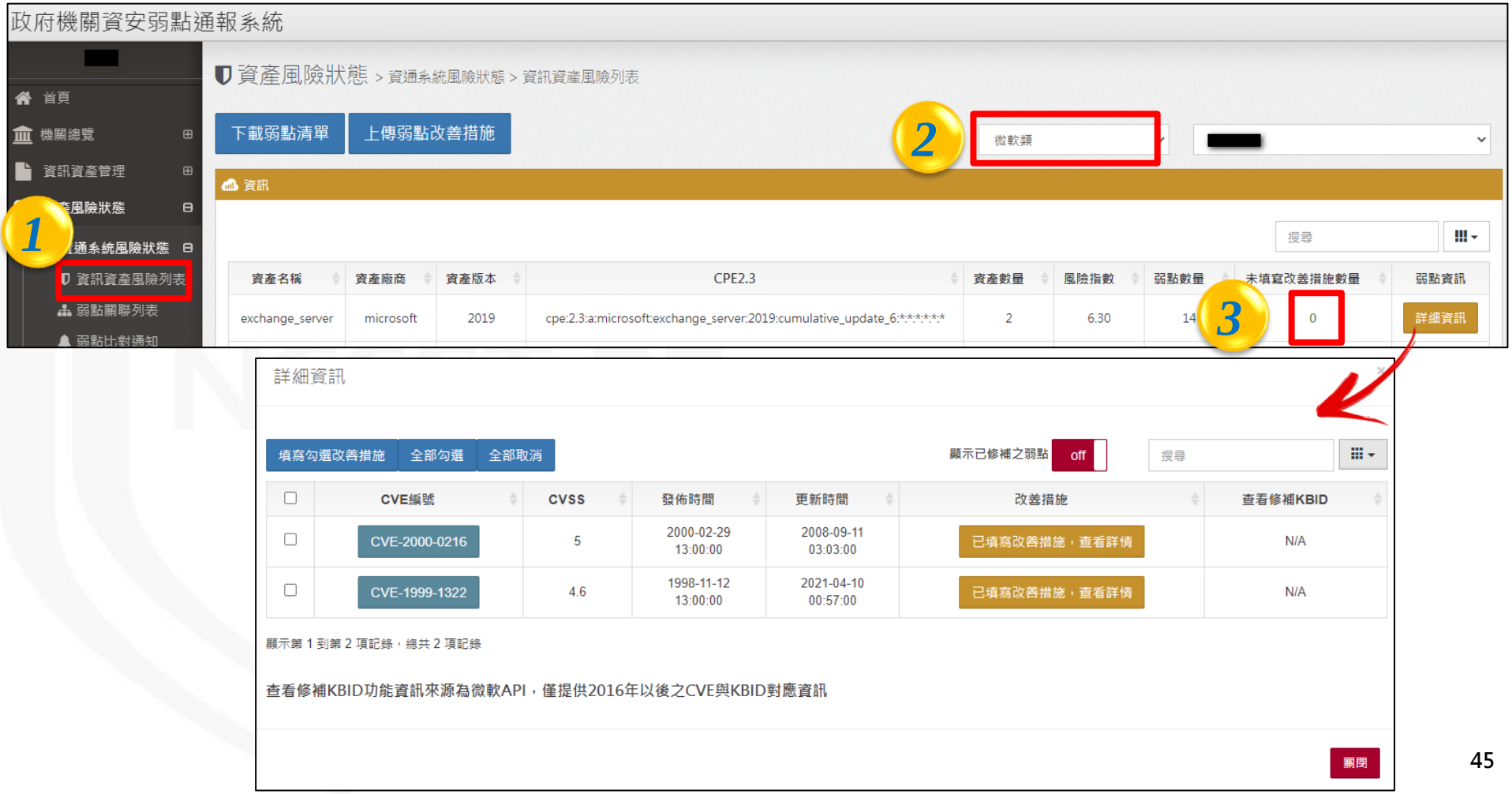
- 以Exchange Server 2019 為例，機關更新KB5000871後，重新盤點已安裝KBID清單，並更新至VANS系統

Upload_KBIDTemplate.xlsx

	A	B	C	D
1	機關OID	機關名稱	已安裝KBID數量	已安裝KBID
2	[redacted]	[redacted]	3	KB4516115
3			2	KB4521863
4			2	KB4528759
5			3	KB4561600
6			2	KB5000871

已安裝KBID更新(2/2)

- VANS系統比對後，Exchange Server 2019所有弱點皆已完成處理



大綱

- 前言
- VANS系統介紹
- VANS系統操作說明
- 預期效益

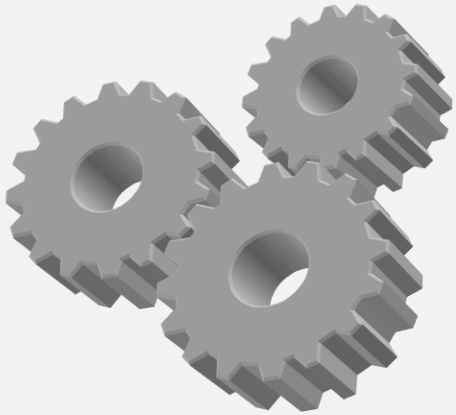
預期效益

- 縮短弱點修補空窗期
  - VANS系統每日更新弱點資料庫(NVD)資料，以提供最新弱點比對結果，當使用軟體存在重大弱點時，機關得以及早得知與應變處理
- 降低重大弱點管控與追蹤之成本
  - 提供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之人力與資源成本
- 追蹤軟體資產弱點修補情形
  - 定時至VANS更新資訊資產項目，完整掌握各項弱點修補情形

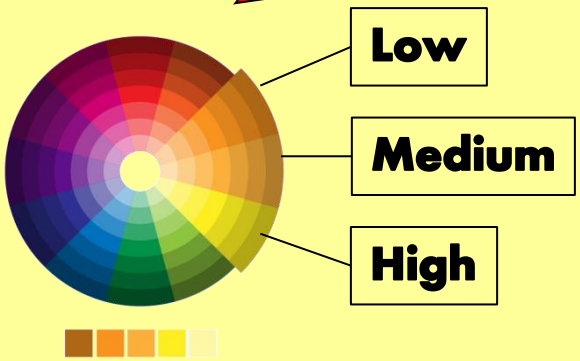
服務維運管理

機關帳號開通

系統與資料維護



提供諮詢與問題排除



持續更新弱點資訊

服務申請流程

聯絡資訊
服務電話：(02)6631-6458
服務信箱：VansService@nccst.nat.gov.tw

申請個人帳號

- 於iAuth系統申請個人帳號

資安人員身分驗證系統(iAuth系統)
https://www.ncert.nat.gov.tw/iAuth2/

機關提出申請

- 於iAuth系統提出VANS權限申請
- 於VANS專區下載並填寫機關管理者帳號申請(異動)單，完成後Email予資安處

技服中心VANS專區
https://www.nccst.nat.gov.tw/Vans?lang=zh

參閱操作手冊

- 操作諮詢
- 服務說明

開始使用服務

- 資料建立
- 弱點比對

VANS系統
https://vans.nccst.nat.gov.tw/

報告完畢
敬請指教

參考資料

- The State of Exploit Development: 80% of Exploits Publish Faster than CVEs
  - https://unit42.paloaltonetworks.com/state-of-exploit-development/
- 政府機關資安弱點通報機制(VANS)專區
  - https://www.nccst.nat.gov.tw/Vans?lang=zh
- 技服中心漏洞警訊公告
  - https://www.nccst.nat.gov.tw/Vulnerability?lang=zh
- National Vulnerability Database(NVD)
  - https://nvd.nist.gov/

附件

API上傳執行方式與格式說明(1/2)

使用者輸入 合作廠商系統自動帶出

- 新增輸入參數

1. api_key (機關API KEY)

(由可視字元組成，長度為88字元)

2. oid (機關OID)
3. unit_name (機關名稱)
4. asset_number (資產數量)
5. product_name (資產名稱)
6. product_vendor (資產廠商)
7. product_version (資產版本)
8. category (資產種類：分為軟體(software)與硬體(hardware)2種)
9. cpe23 (cpe 2.3格式)
10. product_cpename (CPE完整名稱)

範例資料

VANS_API_Sample.json

```
{
    "api_key":"[請輸入API KEY]",
    "data":
[
    {
        "oid": "[請輸入OID]",
        "unit_name": "[請輸入機關名稱]",
        "asset_number": "1",
        "product_name": "Mozilla Firefox 72.0.1 (x64 zh-TW)",
        "product_vendor": "Mozilla",
        "product_version": "72.0.1",
        "category": "software",
        "cpe23": "cpe:2.3:a:mozilla:firefox:72.0.1:*:*:*:*:*:*:*",
        "product_cpename": "Mozilla Firefox 72.0.1"
    },
    {
        "oid": "[請輸入OID]",
        "unit_name": "[請輸入機關名稱]",
        "asset_number": "1",
        "product_name": "MariaDB 10.3 (x64)",
        "product_vendor": "MariaDB Corporation Ab",
        "product_version": "10.3.9.0",
        "category": "software",
        "cpe23": "cpe:2.3:a:mariadb:mariadb:10.3.9:*:*:*:*:*:*:*",
        "product_cpename": "MariaDB 10.3.9"
    }
]
}
```

API上傳執行方式與格式說明(2/2)

- API參數說明

使用者輸入

1. api_key (機關API KEY)

(由可視字元組成，長度為88字元)

合作廠商系統自動帶出

2. oid (機關OID)
3. unit_name (機關名稱)
4. kbid_number (已安裝KBID數量)
5. kbid (已安裝KBID編號)

範例資料

VANS_KBID_Sample.json

```
{
    "api_key":"[請輸入API KEY]",
    "data":
[
    {
        "oid":"[請輸入OID]",
        "unit_name":"請輸入機關名稱",
        "kbid_number":"99",
        "kbid":"KB4565489"
    },
    {
        "oid":"[請輸入OID]",
        "unit_name":"請輸入機關名稱",
        "kbid_number":"123",
        "kbid":"KB4565503"
        }
]
}
```

API回傳代碼格式說明

資訊資產回傳代號	已安裝KBID回傳代號	代號說明	訊息描述說明	資訊資產訊息描述範例	已安裝KBID訊息描述範例
A-S/PC-0101	KB-S/PC-0101	上傳成功	N/A	上傳成功	
A-S/PC-0301	KB-S/PC-0301	API KEY錯誤	N/A	API KEY錯誤	
A-S/PC-0303	KB-S/PC-0303	機關OID錯誤或上傳使用之IP未通過審核	N/A	機關OID錯誤或上傳使用之IP尚未核可	
A-S/PC-0401	KB-S/PC-0401	缺少必要參數	第n筆資料缺少必要參數	1, 3, 7	
A-S/PC-0402	KB-S/PC-0402	機關名稱欄位錯誤	第n筆資料機關名稱欄位錯誤	1, 3, 7	
A-S/PC-0403	KB-S/PC-0403	資產/KBID數量欄位錯誤	第n筆資料資產/KBID數量欄位錯誤	1, 3, 7	
A-S/PC-0404	KB-S/PC-0404	CPE/KBID格式錯誤	第n筆資料CPE/KBID格式錯誤	1, 3, 7	
A-S/PC-0405	KB-S/PC-0405	重複新增相同資產/KBID	單次上傳資料包含重複之資產/KBID	WinRAR 5.50, RARLAB, 5.50, cpe:2.3:a:rarlab:winrar:5.50:*:*:*:*:*:*:*	KB4565483
A-S/PC-0406	KB-S/PC-0406	發生非預期錯誤	N/A	發生非預期錯誤	