分散式弱點管理

分散式弱點管理系統 是雲端應用的弱點管理系統，每一部稽核點除了可以檢測作業系統與應用程式安全弱點外，包含系統狀態以及軟體資產狀態都可以透過遠端的中央控制介面進行遠端排程檢測。藉由中央控制介面匯整分佈在各網路區段中的 Agent 弱點檢測資訊，進而統一管理弱點分佈以及弱點修補與改善狀態

網路型弱點掃描的局限

- 遠端弱點掃描所針對的檢測對象主要為伺服器
- 遠端弱點掃描無法檢測 Client 端應用程式的安全弱點 (如 IE, Firefox, Chrome 等)
- 遠端弱點掃描無法檢測高安全風險的應用程式弱點 (如 Adobe 產品讀取 PDF 檔的 Acrobat ，以及 Flash 播放器, 以及 Oracle Java SE等)
- 通訊埠掃描過程中可能被軟體防火牆阻擋而無法檢測
- Windows 在 Vista 之後(包含Win7/Server2008) ，Remote Registry 預設為 LocalService 啟動，導致無權限進行檢測
- Windows 在 Vista 之後(包含Win7/Server2008) ，微軟已經不再提供以登錄機碼驗證資訊安全更新的方式
- 不屬於網路服務的弱點，無法透過遠端掃描達成檢查

網路型弱點掃描的缺點

遠端檢測 (Remote):

- 沒有 VPN 時，無法檢測用戶的內部網路
- 受防火牆等網路設備影響，無法準確的進行檢測
- 受限於權限，無法完整蒐集系統資訊

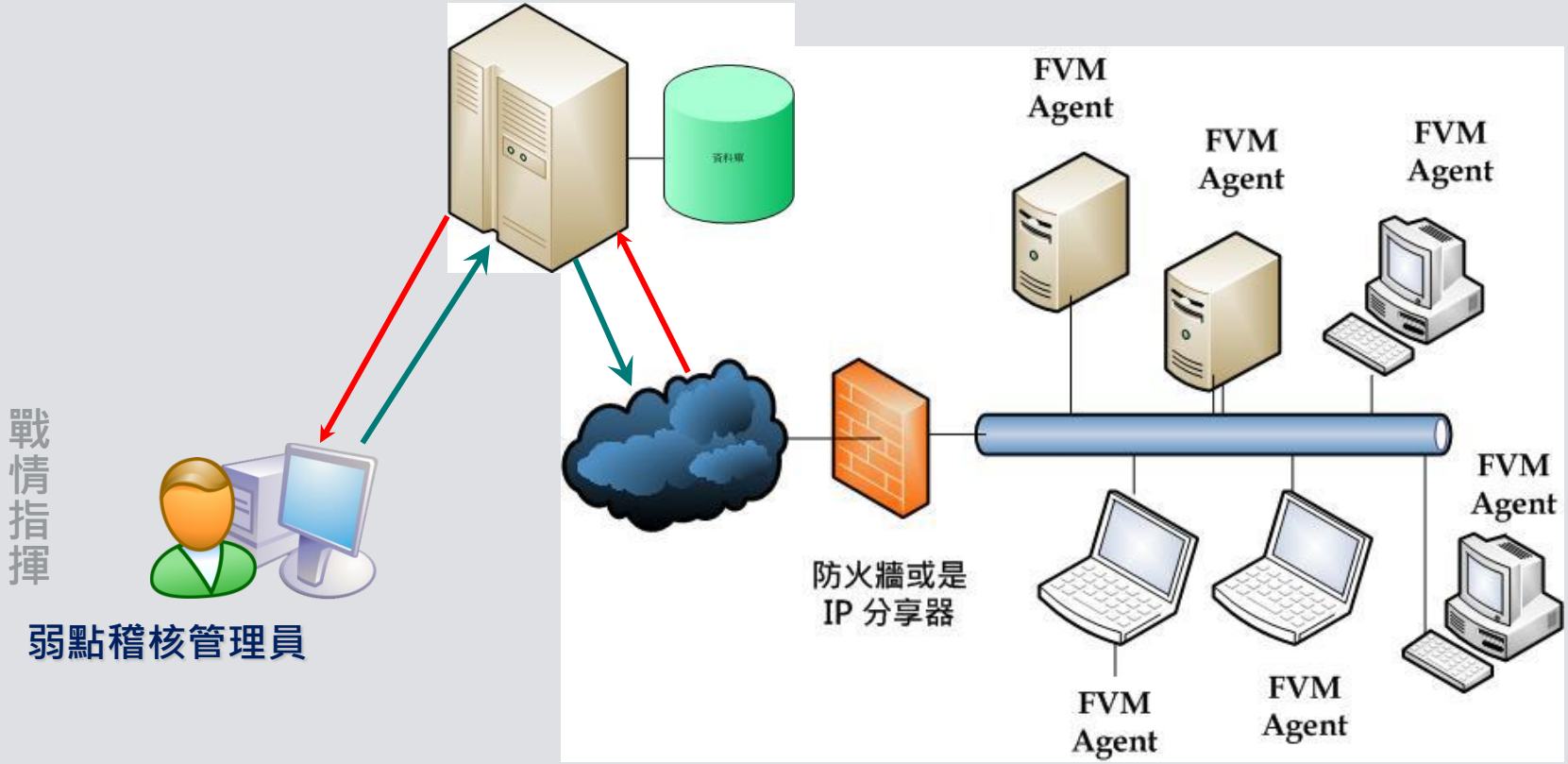
到場檢測 (On-Site):

- 每次檢測都需工程師至用戶端執行檢測，緊盯進度
- 耗費人力、交通、住宿、時間等成本
- 受限於權限，無法完整蒐集系統資訊

甚麼是分散式弱點管理系統?

- 分散式弱點掃描檢測 + 中央集中式管理系統

三層式系統架構 (3-tier)



分散式弱點管理的優勢

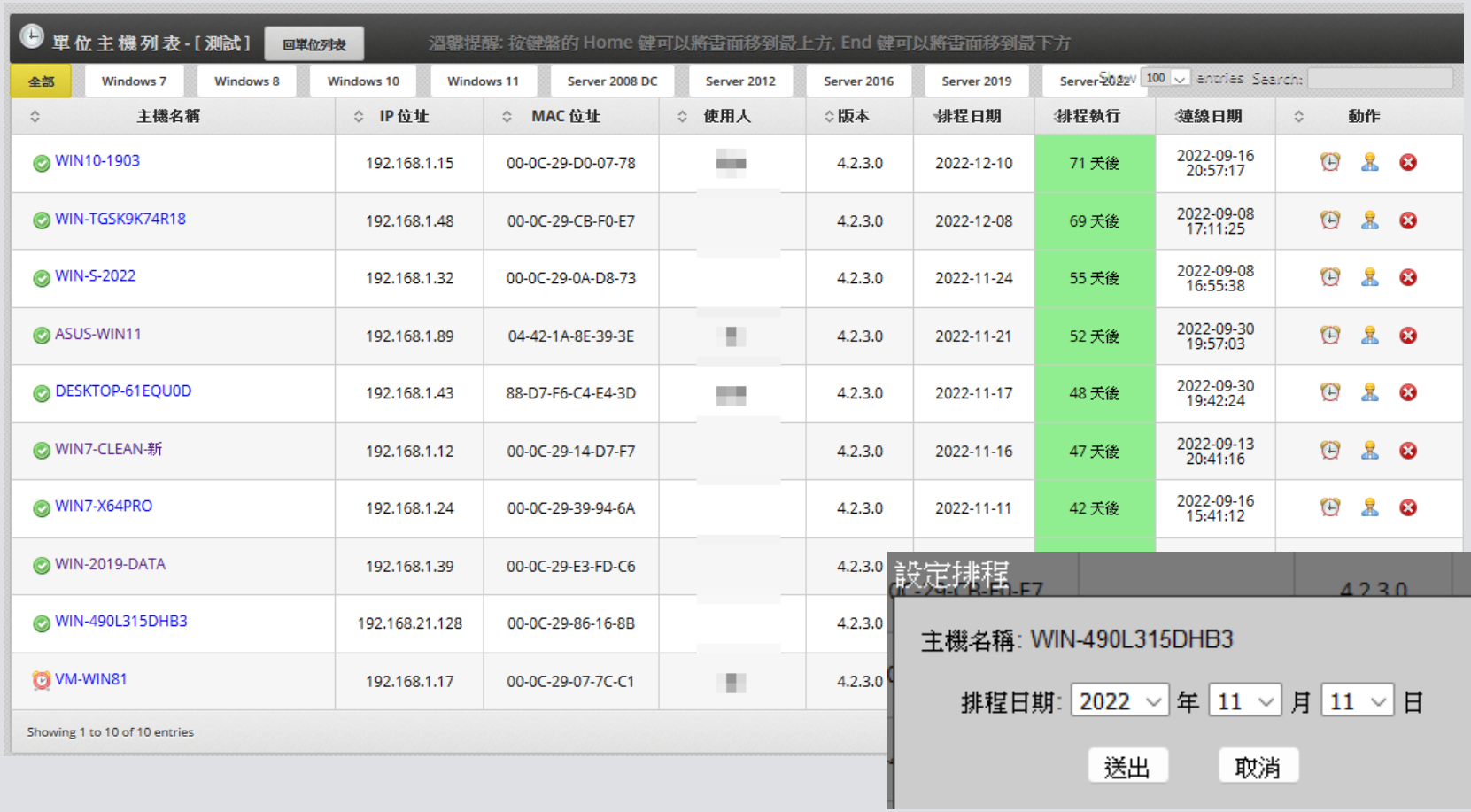
- 三層式系統架構 (3-tier)，不受網路架構限制，能對內網進行稽核 (支援公有雲以及私有雲)
- 分散式佈署: 確保每一部電腦都受到檢測，避免安全疏漏
- 集中式管理: 由管理中心設定一個部門或單一主機於排定的日期自動執行檢測，回傳檢測結果
- 軟體資產管理: 可由軟體清單統計正版軟體，查詢危險惡意軟體
- 檢測結果通知: 檢測完成後，可由管理中心發送電子郵件通知主機使用者，使用者可檢視弱點掃描報告，督促修補弱點
- 使用者也可自行檢測
- 檢測資料儲存於 資料庫，管理中心可客制化查詢與分析等進階應用
- 支援 WebAPI ，可以從另一個管理中心檢視與查詢其他單位的資料

管理中心範例


4MOSAn 分散式弱點管理中心 v2.0 2022-09-30 20:17:25
使用者:
帳號 設定 登出
儀錶板 排程 分析 軟體資產 報表 例外 軟體派送 電腦列表 維護 說明
弱點檢測狀態 (測出弱點項目統計)
140 緊急
91 嚴重
146 高
91 中
205 低
主機排程狀態
1124 總授權數量
16 已使用授權數量
9 已完成檢測主機
7 未完成檢測主機
6 超過 30 天未連線主機
弱點數量
0 50 100 150 200 250
緊急 嚴重 高 中 低
未修補弱點 [嚴重性] 排行
Show 25 entries Search:
數量 嚴重性 CVSS 弱點名稱 弱點類型
1 緊急 10 MS11-083:TCP/IP 中的資訊安全風險可能會允許遠端執行程式碼 (2588516) Windows Hotfix
1 緊急 10 MS12-013:C 執行階段程式庫中的資訊安全風險可能會允許遠端執行程式碼 (2654428) Windows Hotfix
1 緊急 10 MS15-063:Windows 核心中的弱點可能會允許權限提高 (3063858) Windows Hotfix
9 緊急 10 不限制存取光碟 Registry
9 緊急 10 不限制存取軟碟 Registry
9 緊急 10 密碼不會過期 Account
4 緊急 10 密碼最長使用期限太短 Account

管理中心範例

- 從Web介面安排子單位 排程掃描

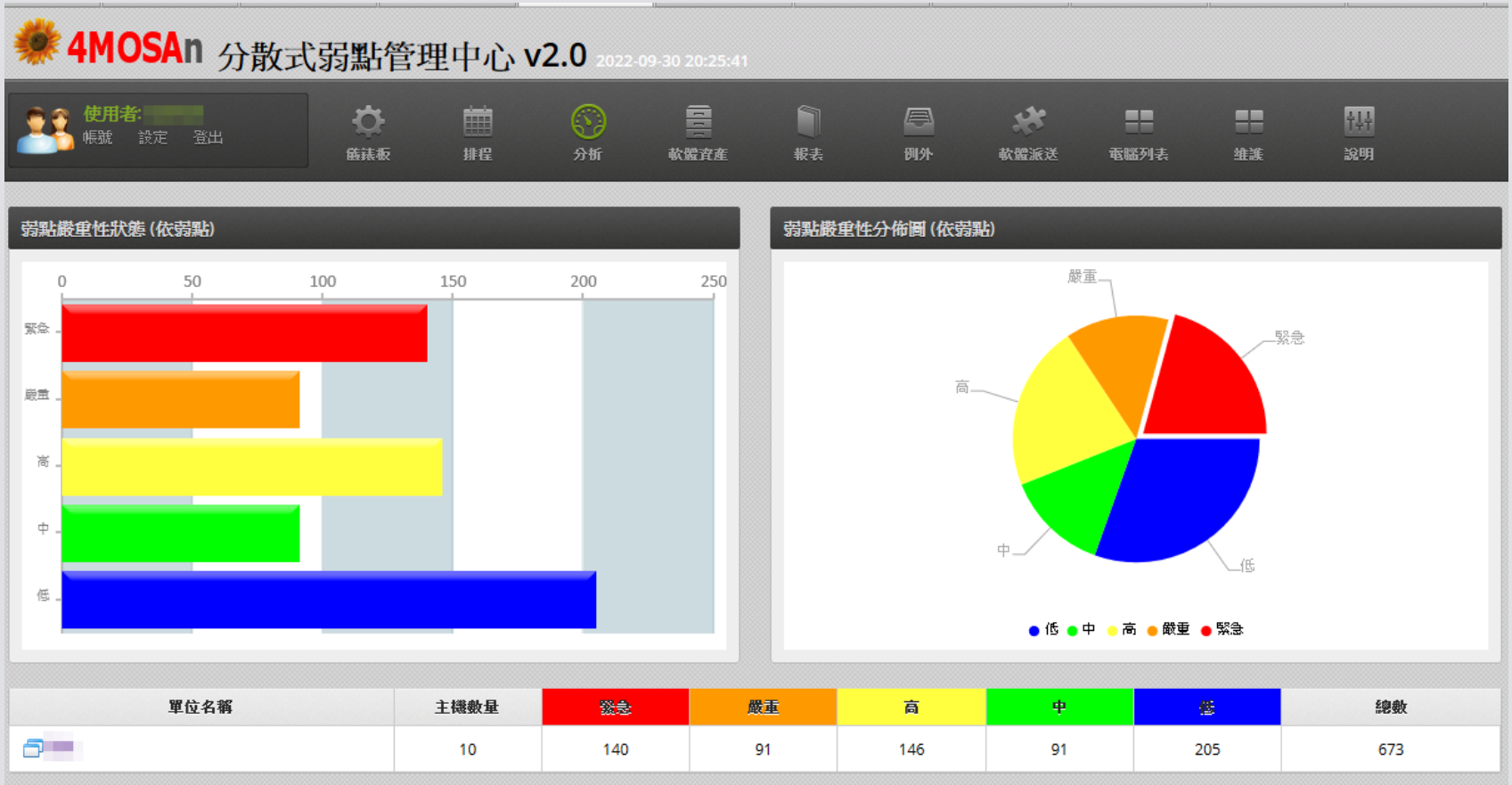


主機資產管理

- 已排程電腦列表匯出與匯入.xlsx (Excel 檔案)

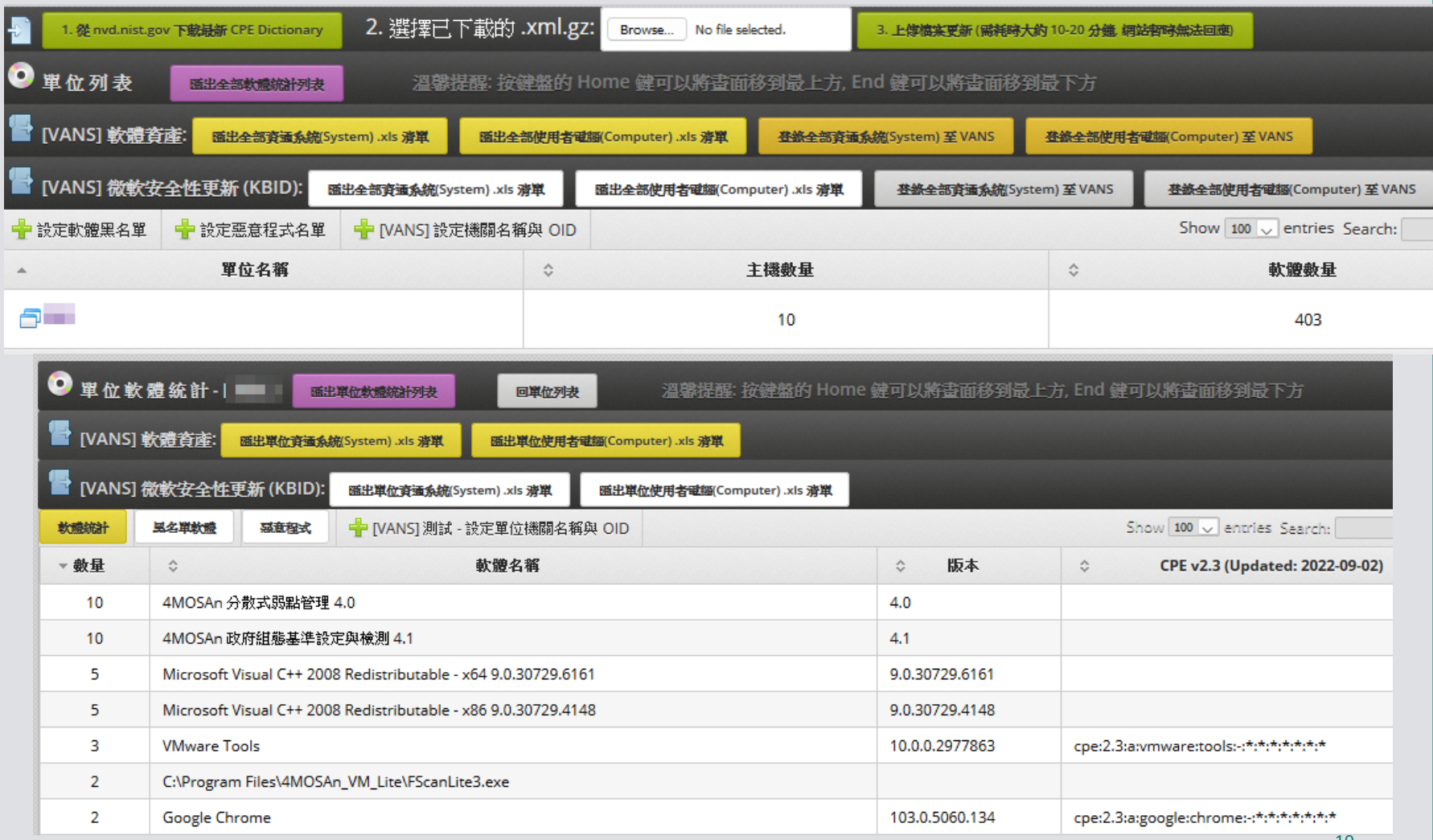
	A	B	C	D	E	F	G	H	I	J	K	L	
1	新主機名稱	單位名稱	使用者姓	e-mail	工作群組	IP 位址	MAC	作業系統	bit	Mainboard	CPU	RAM	HardDisk
2	ASUS-WIN11				HOME	192.168.1.89	04-42-1A-8E-39-3E	Windows 10	64	ASUSTeK COI	11th Gen	16 GByt	磁碟：C 磁
3	DESKTOP-61EQU0D				WORKGROUP	192.168.1.43	88-D7-F6-C4-E4-3D	Windows 10	64	ASUSTeK COI	AMD Ryz	32 GByt	磁碟：C 磁
4	VM-WIN81				HOME	192.168.1.17	00-0C-29-07-7C-C1	Windows 8.1	32	VMware, Inc	11th Gen	1 GByte	磁碟：C 磁
5	WIN-2019-DATA				HOME	192.168.1.39	00-0C-29-E3-FD-C6	Windows Se	64	VMware, Inc	11th Gen	8 GByte	磁碟：C 磁
6	WIN-490L315DHB3				WORKGROUP	192.168.21.128	00-0C-29-86-16-8B	Windows Se	64	VMware, Inc	11th Gen	2 GByte	磁碟：C 磁
7	WIN-S-2022				WORKGROUP	192.168.1.32	00-0C-29-0A-D8-73	Windows Se	64	VMware, Inc	11th Gen	2 GByte	磁碟：C 磁
8	WIN-TGSK9K74R18				WORKGROUP	192.168.1.48	00-0C-29-CB-F0-E7	Windows Se	64	VMware, Inc	11th Gen	2 GByte	磁碟：C 磁
9	WIN10-1903				HOME	192.168.1.15	00-0C-29-D0-07-78	Windows 10	64	VMware, Inc	11th Gen	2 GByte	磁碟：C 磁
10	WIN7-CLEAN-新				HOME	192.168.1.12	00-0C-29-14-D7-F7	Windows 7 F	32	VMware, Inc	11th Gen	1 GByte	磁碟：C 磁
11	WIN7-X64PRO				HOME	192.168.1.24	00-0C-29-39-94-6A	Windows 7 F	64	VMware, Inc	11th Gen	2 GByte	磁碟：C 磁

管理中心-分析



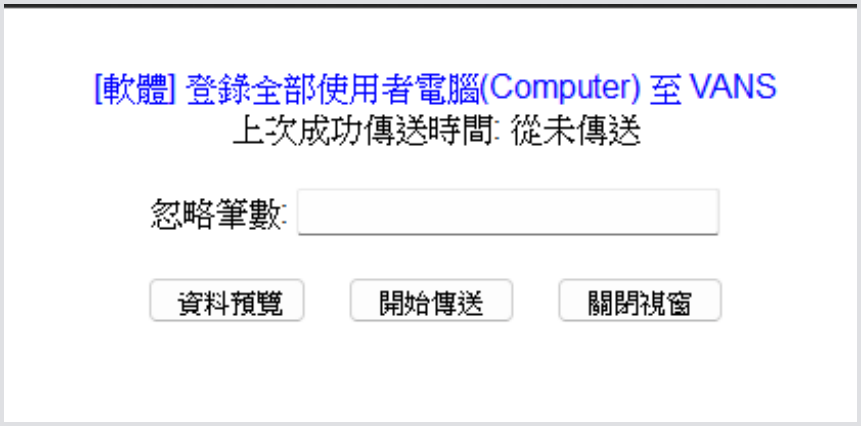
單位名稱	主機數量	緊急	嚴重	高	中	低	總數
	10	140	91	146	91	205	673

管理中心-軟體資產


1. 從 nvd.nist.gov 下載最新 CPE Dictionary
2. 選擇已下載的 .xml.gz:
Browse...
No file selected.
3. 上傳檔案更新 (需耗時大約 10-20 分鐘 網站暫時無法回應)
單位列表
匯出全部軟體統計列表
溫馨提醒: 按鍵盤的 Home 鍵可以將畫面移到最上方, End 鍵可以將畫面移到最下方
[VANS] 軟體資產:
匯出全部資通系統(System) .xls 清單
匯出全部使用者電腦(Computer) .xls 清單
登錄全部資通系統(System) 至 VANS
登錄全部使用者電腦(Computer) 至 VANS
[VANS] 微軟安全性更新 (KBID):
匯出全部資通系統(System) .xls 清單
匯出全部使用者電腦(Computer) .xls 清單
登錄全部資通系統(System) 至 VANS
登錄全部使用者電腦(Computer) 至 VANS
設定軟體黑名單
設定惡意程式名單
[VANS] 設定機關名稱與 OID
Show 100 entries Search:
單位名稱
主機數量
軟體數量
10
403
單位軟體統計 - [redacted]
匯出單位軟體統計列表
回單位列表
溫馨提醒: 按鍵盤的 Home 鍵可以將畫面移到最上方, End 鍵可以將畫面移到最下方
[VANS] 軟體資產:
匯出單位資通系統(System) .xls 清單
匯出單位使用者電腦(Computer) .xls 清單
[VANS] 微軟安全性更新 (KBID):
匯出單位資通系統(System) .xls 清單
匯出單位使用者電腦(Computer) .xls 清單
軟體統計
黑名單軟體
惡意程式
[VANS] 測試 - 設定單位機關名稱與 OID
Show 100 entries Search:
數量
軟體名稱
版本
CPE v2.3 (Updated: 2022-09-02)
10 4MOSAn 分散式弱點管理 4.0 4.0
10 4MOSAn 政府組態基準設定與檢測 4.1 4.1
5 Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 9.0.30729.6161
5 Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 9.0.30729.4148
3 VMware Tools 10.0.0.2977863 cpe:2.3:a:vmware:tools:-:*:*:*:*:*:*:*
2 C:\Program Files\4MOSAn_VM_Lite\FScanLite3.exe
2 Google Chrome 103.0.5060.134 cpe:2.3:a:google:chrome:-:*:*:*:*:*:*:*

管理中心-軟體資產

- 支援技服資通安全弱點通報機制(VANS)
- 軟體資產 與 微軟安全性更新 (KBID):
- 匯出 .xls 清單 與 WebAPI 登錄 (可預覽資料)



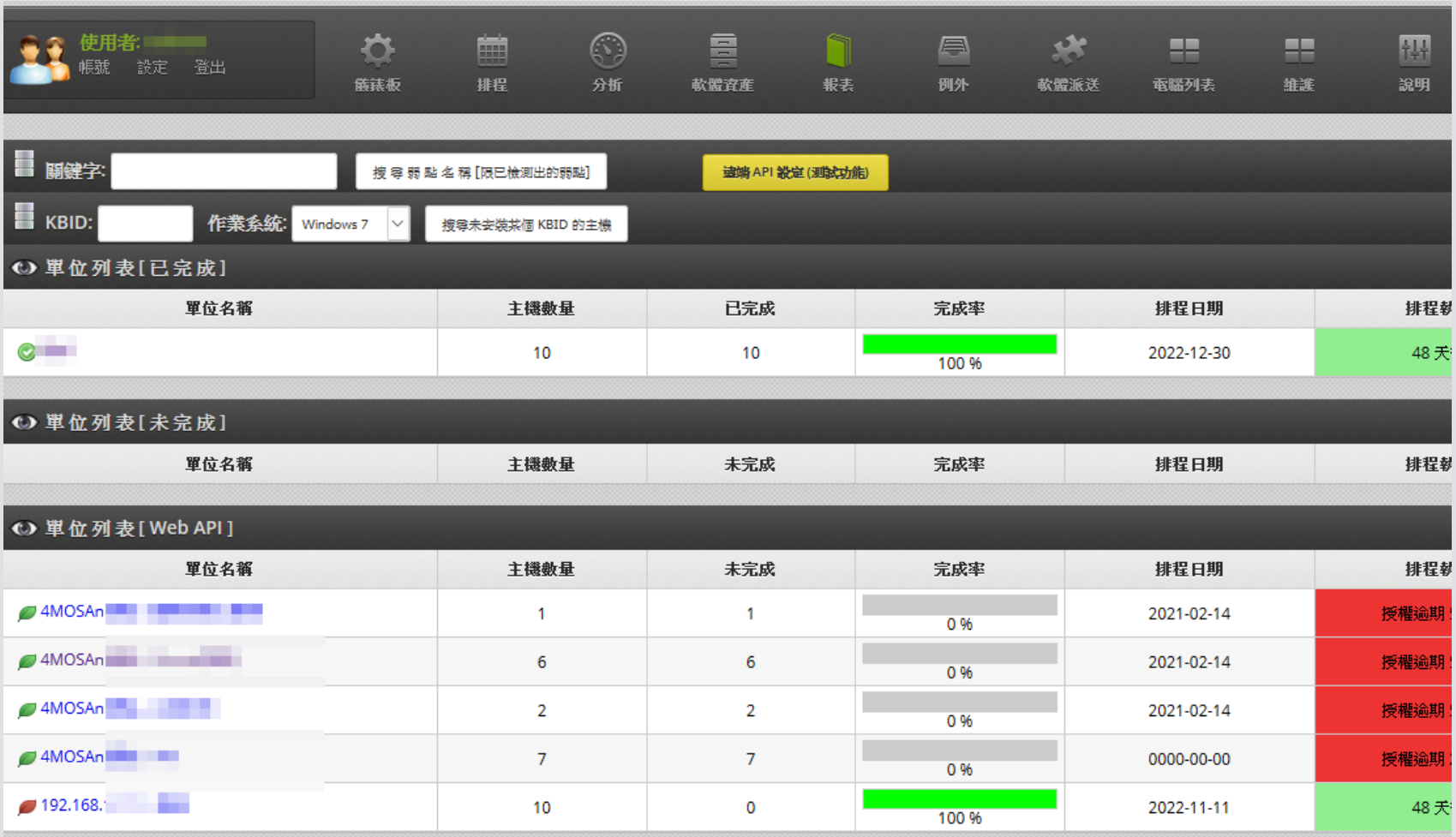
- 可設定 軟體黑名單
- 可設定惡意程式名單 (軟體路徑與檔案名稱)
- 可匯出軟體統計列表 .xls (包含軟體存在於那些主機上, 可清查)

註: VANS .xls 清單不包含主機資訊, 無法清查

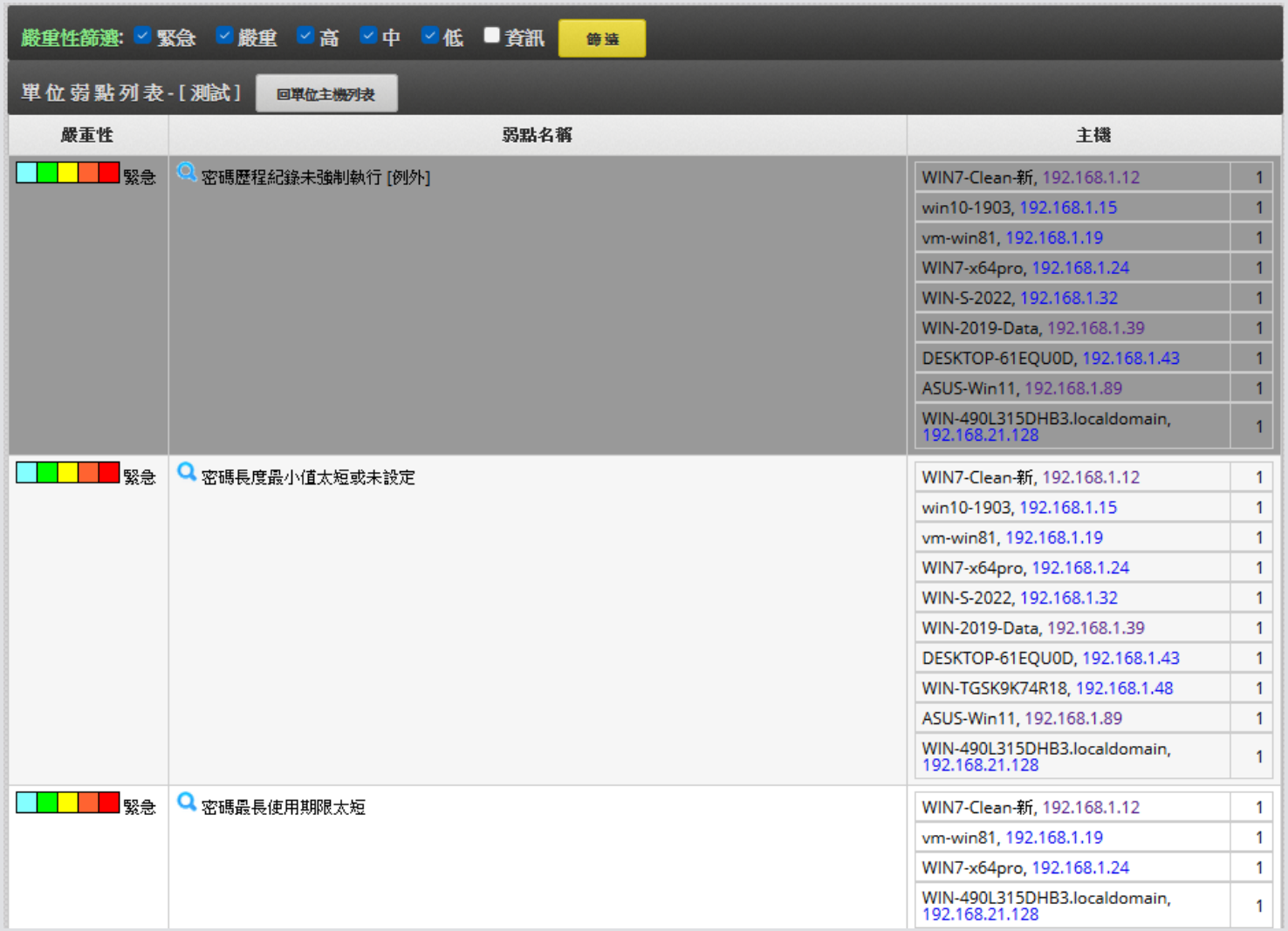
管理中心-軟體資產-VANS 預覽


```
api_key:
data:
  0:
    oid:              "vendorJ8L1"
    unit_name:        "VANS測試機關9"
    asset_number:     "2"
    product_name:     "Windows 10 Home 2009 (21H2) x64"
    product_vendor:   "Microsoft Corporation"
    product_version:  "20h2"
    category:         "software"
    cpe23:            "cpe:2.3:o:microsoft:windo…_10:20h2:*:*:*:*:*:x64:*"
    product_cpename:  "Microsoft Windows 10 20H2 on x64"
  1:
    oid:              "vendorJ8L1"
    unit_name:        "VANS測試機關9"
    asset_number:     "1"
    product_name:     "Windows 10 Pro 1909 x64"
    product_vendor:   "Microsoft Corporation"
    product_version:  "1909"
    category:         "software"
    cpe23:            "cpe:2.3:o:microsoft:windo…_10:1909:*:*:*:*:*:x64:*"
    product_cpename:  "Microsoft Windows 10 1909 64-bit"
```

管理中心-稽核報告


使用者:
帳號 設定 登出
儀表板
排程
分析
軟體資產
報表
例外
軟體派送
電腦列表
維護
說明
關鍵字:
搜尋弱點名稱[限已檢測出的弱點]
遠端API設定(測試功能)
KBID:
作業系統:
Windows 7
搜尋未安裝某個KBID的主機
單位列表[已完成]
單位名稱 主機數量 已完成 完成率 排程日期 排程
10 10 100 % 2022-12-30 48 天
單位列表[未完成]
單位名稱 主機數量 未完成 完成率 排程日期 排程
單位列表[Web API]
單位名稱 主機數量 未完成 完成率 排程日期 排程
4MOSAn 1 1 0 % 2021-02-14 授權逾期
4MOSAn 6 6 0 % 2021-02-14 授權逾期
4MOSAn 2 2 0 % 2021-02-14 授權逾期
4MOSAn 7 7 0 % 0000-00-00 授權逾期
192.168. 10 0 100 % 2022-11-11 48 天

管理中心-稽核報告-弱點統計



管理中心-稽核報告-弱點統計

嚴重性篩選: ☑ 緊急 ☑ 嚴重 ☑ 高 ☑ 中 ☑ 低 ☐ 資訊 篩選

單位弱點列表-[測試] 回單位主機列表

嚴重性	弱點名稱	主機	
緊急	MS14-043:Windows Media Center 中的資訊安全風險可能會允許遠端執行程式碼 (2978742)	WIN7-Clean-新, 192.168.1.12	1
緊急	MS14-074:遠端桌面通訊協定中的資訊安全風險可能會允許略過資訊安全功能 (3003743)	WIN7-Clean-新, 192.168.1.12	1
		vm-win81, 192.168.1.19	1
		WIN-490L315DHB3.localdomain, 192.168.21.128	1
緊急	MS15-034:HTTP.sys 中的資訊安全風險可能會允許遠端執行程式碼 (3042553)	WIN7-Clean-新, 192.168.1.12	1
		vm-win81, 192.168.1.19	1
		WIN-490L315DHB3.localdomain, 192.168.21.128	2
緊急	MS15-060:Microsoft 通用控制項中的弱點可能會允許遠端執行程式碼 (3059317)	vm-win81, 192.168.1.19	1
		WIN-490L315DHB3.localdomain, 192.168.21.128	1
緊急	MS15-063:Windows 核心中的弱點可能會允許權限提高 (3063858)	WIN7-Clean-新, 192.168.1.12	1
緊急	MS15-068:Windows Hyper-V 中的資訊安全風險可能會允許遠端執行程式碼 (3072000)	WIN-490L315DHB3.localdomain, 192.168.21.128	1
緊急	MS15-075:OLE 中的資訊安全風險可能會允許提高權限 (3072633)	WIN7-Clean-新, 192.168.1.12	1
		vm-win81, 192.168.1.19	1
		WIN-490L315DHB3.localdomain, 192.168.21.128	1
緊急	MS15-082:RDP 中的弱點會允許遠端程式碼執行 (3080348)	vm-win81, 192.168.1.19	1
		WIN-490L315DHB3.localdomain, 192.168.21.128	1

管理中心: 報表-主機歷史紀錄

- 自動留存每一次弱點掃描的歷史紀錄

單位主機列表-[| WIN-2019-DATA 回上一頁

最新完成的檢測

選擇	IP 位址	主機名稱	作業系統	防毒軟體名稱	弱點數	Hotfix	完成檢測
修補 檢視 刪除	192.168.1.43	WIN-2019-Data	Server 2019 Datacenter 1809 Build 17763 (x64)	作業系統不支援	27	9	2022-10-01 16:38:34

之前的檢測

選擇	IP 位址	主機名稱	作業系統	防毒軟體名稱	弱點數	Hotfix	完成檢測
修補 檢視 刪除	192.168.1.39	WIN-2019-Data	Server 2019 Datacenter 1809 Build 17763 (x64)	作業系統不支援	28	9	2022-08-12 20:50:54
修補 檢視 刪除	192.168.1.39	WIN-2019-Data	Server 2019 Datacenter 1809 Build 17763 (x64)	作業系統不支援	27	9	2022-07-29 16:15:31

[維護] 刪除舊資料 只保留一年以內的紀錄

管理中心: 報表-主機-弱點稽核

HTML 報表 | PDF 報表 | 報表選項: 統計圖表 通訊埠 Windows 帳號 Windows 服務 軟體資產 網芳分享 工作檢核表

主機詳細資料 - [測試] WIN-2019-Data : 192.168.1.43 - 2022-10-01 16-38-34 | 回上一頁

弱點稽核 | 通訊埠 | Windows 帳號 | Windows 服務 | 軟體資產 | 處理程序 | 網芳分享 | Hotfix | 檢測資訊

弱點稽核

Num	嚴重性	CVSS	弱點名稱	弱點類型
1	緊急	7	密碼歷程紀錄未強制執行 [例外]	Account
2	緊急	10	密碼長度最小值太短或未設定	Account
3	緊急	10	密碼不會過期	Account
4	緊急	10	不限制存取光碟	Registry
5	緊急	10	密碼超過最長有效期	Account
6	緊急	10	不限制存取軟碟	Registry
7	嚴重	7.2	危險的 Windows AutoRun	Registry
20	低	2.1	預設的管理員帳號	Account
21	低	2.1	分頁檔案未清除	Registry
22	低	2.1	預設的來賓帳戶名稱	Account
23	高	5	KB890830：Windows 惡意軟體移除工具 x64 - v5.94	Windows Hotfix
24	低	2	Microsoft Defender Antivirus 安全智能更新 - KB2267602（版本 1.371.1024.0）	Windows Hotfix
25	低	2	2020-07 適用於 x64 系統 Windows Server 2019 (1809) 的累積更新 (KB4558998)	Windows Hotfix
26	低	2	更新以移除 x64 型系統的 Windows Server 2019 Adobe Flash Player (KB4577586)	Windows Hotfix
27	低	2	2022-02 適用於 x64 系統之 Windows Server 2019 的 .NET Framework 3.5、4.7.2 和 4.8 的累積更新預覽 (KB5011267)	Windows Hotfix

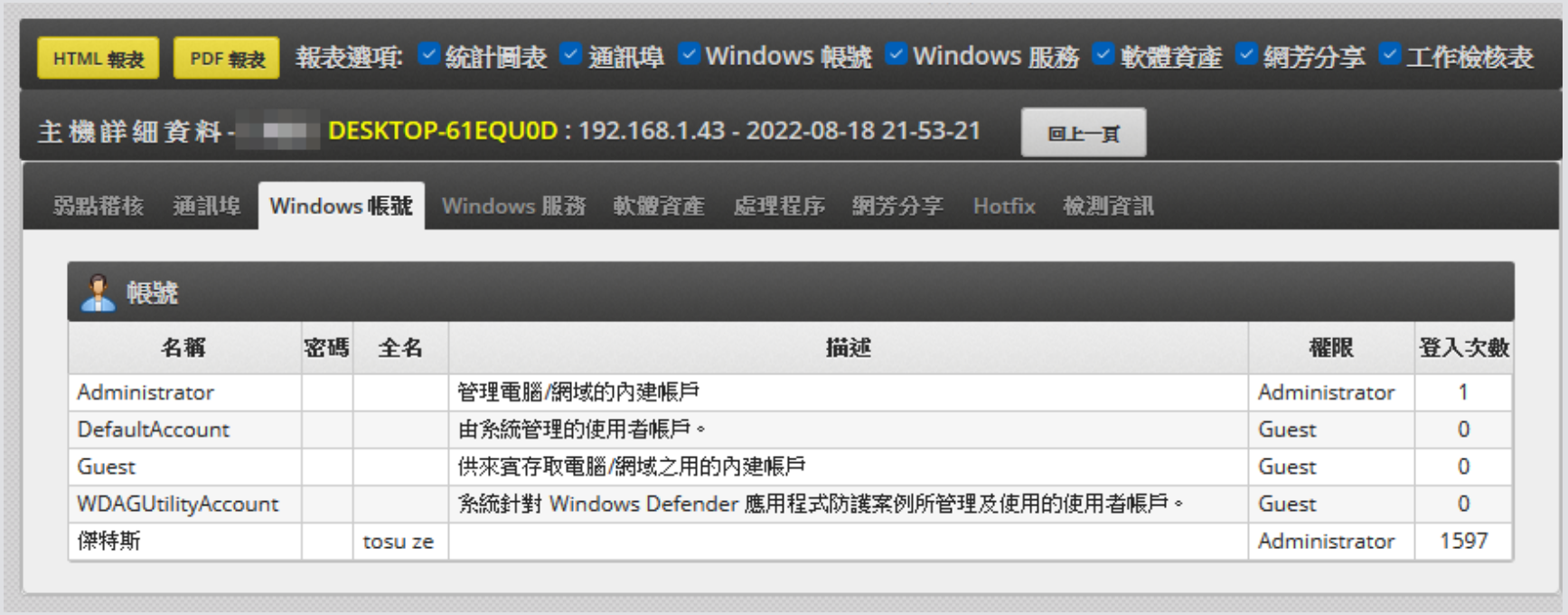
管理中心: 報表-主機-通訊埠

弱點稽核 | 通訊埠 | Windows 帳號 | Windows 服務 | 軟體資產 | 處理程序 | 網芳分享 | Hotfix | 檢測資訊

通訊埠

通訊埠	描述	回應內容	弱點稽核
135	Microsoft Remote Procedure Call (RPC) service		10
137	NETBIOS Name Service	MAC Address: 00-0C-29-14-D7-F7 NIC Vendor: VMware, Inc. Name Table: WIN7-CLEAN-s <0><UNIQUE> HOME <0><GROUP> HOME <1E><GROUP> WIN7-CLEAN-s <20><UNIQUE> Probe Hex: \x04\x80\xF0\x84\x00\x00\x00\x00\x01\x00\x00\x00\x00\x20\x43\x4B \x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41 \x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x00\x00 \x21\x00\x01\x00\x00\x00\x00\x00\x77\x04\x57\x49\x4E\x37\x2D\x43 \x4C\x45\x41\x4E\x2D\xB7\x73\x20\x20\x00\x04\x00\x48\x4F\x4D\x45 \x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x00\x84\x00\x48\x4F \x4D\x45\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x1E\x84\x00 \x57\x49\x4E\x37\x2D\x43\x4C\x45\x41\x4E\x2D\xB7\x73\x20\x20\x20 \x04\x00\x00\x0C\x29\x14\xD7\xF7\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 Probe Text: ..... CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..!.....w.WIN7-CLEAN-.s ...HOME ...HOME ...WIN7-CLEAN-.s ....).....	1
139	NETBIOS Session Service		0
445	Microsoft-DS	Native OS: Windows 7 Professional 7601 Service Pack 1 Native LAN Manager: Windows 7 Professional 6.1	0

管理中心: 報表-主機-帳號



名稱	密碼	全名	描述	權限	登入次數
Administrator			管理電腦/網域的內建帳戶	Administrator	1
DefaultAccount			由系統管理的使用者帳戶。	Guest	0
Guest			供來賓存取電腦/網域之用的內建帳戶	Guest	0
WDAGUtilityAccount			系統針對 Windows Defender 應用程式防護案例所管理及使用的使用者帳戶。	Guest	0
傑特斯		tosu ze		Administrator	1597

管理中心: 報表-主機-服務

弱點稽核 | 通訊埠 | Windows 帳號 | Windows 服務 | 軟體資產 | 處理程序 | 網芳分享 | Hotfix | 檢測資訊

服務

名稱	描述	狀態	啟動類型	執行檔所在路徑
AarSvc_c76f6	Agent Activation Runtime_c76f6	已啟動	手動	C:\WINDOWS\system32\svchost.exe -k AarSvcGroup -p
AJRouter	AllJoyn Router Service		手動	C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p
ALG	Application Layer Gateway Service		手動	C:\WINDOWS\System32\alg.exe
AppIDSvc	Application Identity		手動	C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Appinfo	Application Information	已啟動	手動	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
AppMgmt	Application Management		手動	C:\WINDOWS\system32\svchost.exe -k netsvcs -p
AppReadiness	App Readiness		手動	C:\WINDOWS\System32\svchost.exe -k AppReadiness -p
AppVClient	Microsoft App-V Client		停用	C:\WINDOWS\system32\AppVClient.exe
AppXSvc	AppX Deployment Service (AppXSVC)	已啟動	手動	C:\WINDOWS\system32\svchost.exe -k wsappx -p
AssignedAccessManagerSvc	AssignedAccessManager 服務		手動	C:\WINDOWS\system32\svchost.exe -k AssignedAccessManagerSvc
AudioEndpointBuilder	Windows Audio Endpoint Builder	已啟動	自動	C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Audiosrv	Windows Audio	已啟動	自動	C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p
autotimesvc	行動電話通訊的時間		手動	C:\WINDOWS\system32\svchost.exe -k autoTimeSvc
AVP21.3	卡巴斯基防毒軟體服務 21.3	已啟動	自動	"C:\Program Files (x86)\Kaspersky Lab\Kaspersky Free 21.3\avp.exe" -r
AxInstSV	ActiveX Installer (AxInstSV)		手動	C:\WINDOWS\system32\svchost.exe -k AxInstSVGroup

管理中心: 報表-主機-軟體資產

弱點稽核 | 通訊埠 | Windows 帳號 | Windows 服務 | 軟體資產 | 處理程序 | 網芳分享 | Hotfix | 檢測資訊

軟體資產

名稱	版本
Tools for .Net 3.5	3.11.50727
Tools for .Net 3.5 - CHT Lang Pack	3.11.50727
${{arpDisplayName}}	11.6
4MOSAn 分散式弱點管理 4.0	4.0
4MOSAn 政府組態基準設定與檢測 4.1	4.1
Adobe Photoshop CS6	13.0
AdobePDFSettings11-new-ja_JP	11.0
Bamboo	5.2.4-6
Bandizip	7.09
Blackmagic RAW Common Components	2.4.0.1
Blender	
BlueStacks App Player	4.280.0.1022
Camera (NVIDIA Broadcast)	1.3.0.45
CHM Editor	3.2.0
Chrome Remote Desktop Host	105.0.5195.5
Compute Sanitizer	11.6
CosmicBreak Universal	
CUBLAS Development	11.6
CUBLAS Runtime	11.6
CUDA CCCL	11.6
CUDA Documentation	11.6
CUDA Profiler Tools	11.6
CUDA Toolkit	11.6
CUDART Runtime	11.6
CUFFT Development	11.6

管理中心: 報表-主機-程序與分享

弱點稽核 | 通訊埠 | Windows 帳號 | Windows 服務 | 軟體資產 | 處理程序 | 網芳分享 | Hotfix | 檢測資訊

處理程序

程序列表
C:\Program Files (x86)\4MOSAn_VM_Lite\FScanLite3.exe
C:\Program Files (x86)\4MOSAn_VM_Lite\FVMSVC.exe
C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe
C:\Program Files (x86)\Common Files\Steam\SteamService.exe
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe
C:\Program Files (x86)\EasyAntiCheat_EOS\EasyAntiCheat_EOS.exe
C:\Program Files (x86)\Google\Chrome Remote Desktop\105.0.5195.5\remoting_host.exe
C:\Program Files (x86)\Google\Chrome Remote Desktop\105.0.5195.5\remoting_host.exe
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler.exe
C:\Program Files (x86)\Google\Update\1.3.36.132\GoogleCrashHandler64.exe
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Free 21.3\avp.exe
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Free 21.3\avpui.exe
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Free 21.3\plugins_nms.exe
C:\Program Files (x86)\LogMeIn Hamachi\hamachi-2-ui.exe

網芳分享

名稱	描述	密碼
ADMIN$	遠端管理	
C$	預設共用	
E$	預設共用	
F$	預設共用	
G$	預設共用	
IPC$	遠端 IPC	

管理中心: 報表-主機-已安裝KBID

弱點稽核 | 通訊埠 | Windows 帳號 | Windows 服務 | 軟體資產 | 處理程序 | 網芳分享 | Hotfix | 檢測資訊

Hotfix

名稱	KBID
MS06-061:MSXML 6.0 RTM 安全性更新程式 (925673)	KB925673
MS11-025:Microsoft Visual C++ 2005 Service Pack 1 可轉散發套件的安全性更新 (KB2538242)	KB2538242
MS11-025:Microsoft Visual C++ 2008 Service Pack 1 可轉散發套件的安全性更新 (KB2538243)	KB2538243
MS11-025:Microsoft Visual C++ 2010 Service Pack 1 可轉散發套件的安全性更新 (KB2565063)	KB2565063
Microsoft Office 2010 更新 (KB2553092)，64 位元版	KB2553092
Microsoft Office 2010 (KB2687455) 64 位元版本 Service Pack 2	KB2687455
Microsoft Office 2010 (KB2825640) 64 位元版本 的更新	KB2825640
Microsoft Office 2010 (KB2589298) 64 位元版本 的更新	KB2589298
Microsoft Office 2010 (KB2589375) 64 位元版本 的更新	KB2589375
Microsoft Office 2010 (KB2597087) 64 位元版本 的更新	KB2597087
MS13-106:Microsoft Office 2010 (KB2850016) 64 位元版本 的安全性更新	KB2850016
Microsoft InfoPath 2010 (KB2817369) 64 位元版本 的更新	KB2817369
Microsoft SharePoint Workspace 2010 (KB2760601) 64 位元版本 的更新	KB2760601
MS14-024:Microsoft Office 2010 (KB2880971) 64 位元版本 的安全性更新	KB2880971
Microsoft Office 2010 (KB2589386) 64 位元版本 的更新	KB2589386
Microsoft Office 2010 (KB2883019) 64 位元版本 的更新	KB2883019
Microsoft Office 2010 (KB2553140) 64 位元版本 的更新	KB2553140
MS15-013:Microsoft Office 2010 (KB2920748) 64 位元版本 的安全性更新	KB2920748
MS15-022:Microsoft Office 2010 (KB2956076) 64 位元版本 的安全性更新	KB2956076
Microsoft Outlook Social Connector 2010 (KB2553308) 64 位元版本 的更新	KB2553308
Microsoft Office 2010 (KB2553347) 64 位元版本 的更新	KB2553347
Microsoft Office 2010 (KB3054873) 64 位元版本 的更新	KB3054873

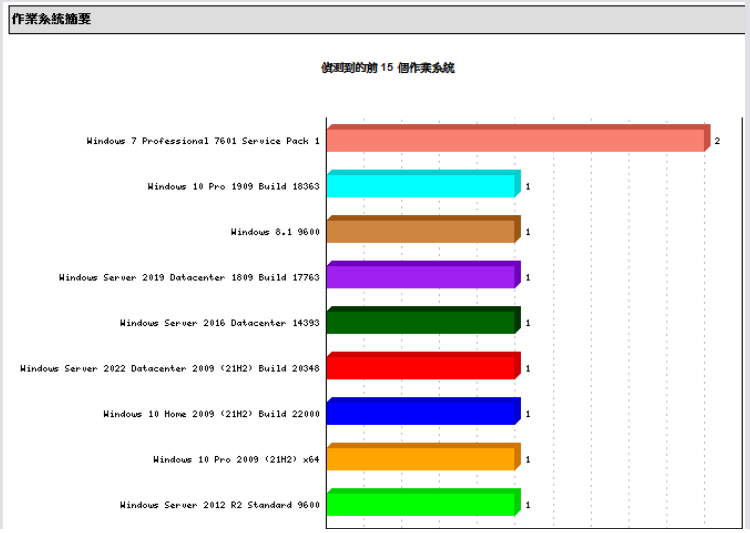
管理中心: 報表-主機-檢測資訊

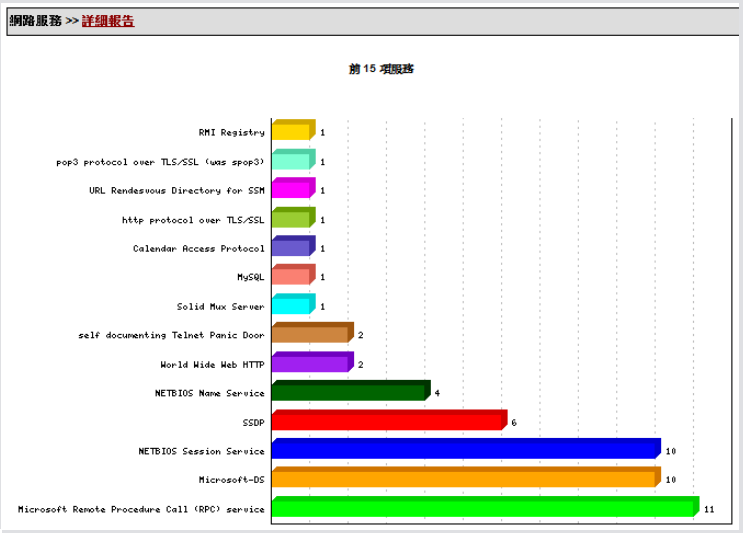
整體統計
管理報告與技術報告

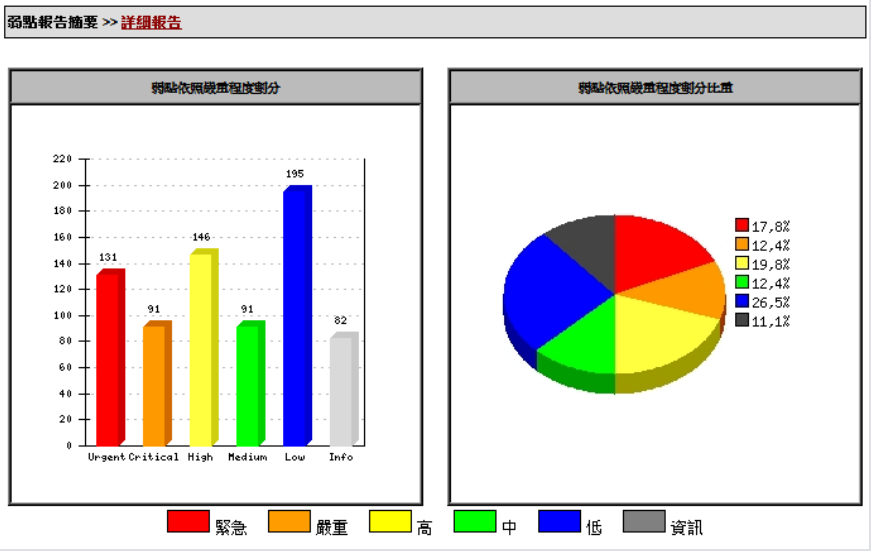
4MOSAn

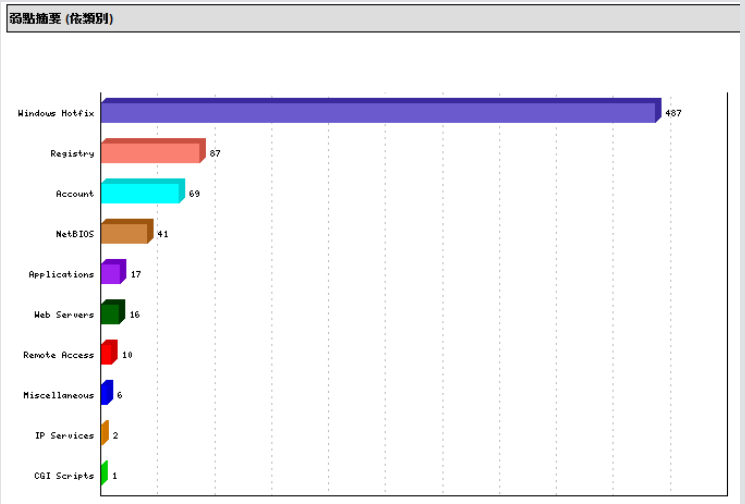
美麗島安全科技

管理報告包含多種統計圖表









管理報告包含整體統計

DNS 名稱 NetBios 名稱 標籤	IP 位址	作業系統	服務	唯一弱點
win10-1903	192.168.1.15	Windows 10 Pro 1909 Build 18363	TCP - 135 TCP - 139 TCP - 445	34
WIN7-x64pro	192.168.1.24	Windows 7 Professional 7601 Service Pack 1	TCP - 135 UDP - 137 TCP - 139 TCP - 445 UDP - 1900	101
WIN-2019-Data	192.168.1.43	Windows Server 2019 Datacenter 1809 Build 17763	TCP - 135 TCP - 139 TCP - 445 UDP - 1900	35
vm-win81	192.168.1.19	Windows 8.1 9600	TCP - 135 UDP - 137 TCP - 139 TCP - 445 UDP - 1900	110

管理報告包含整體統計

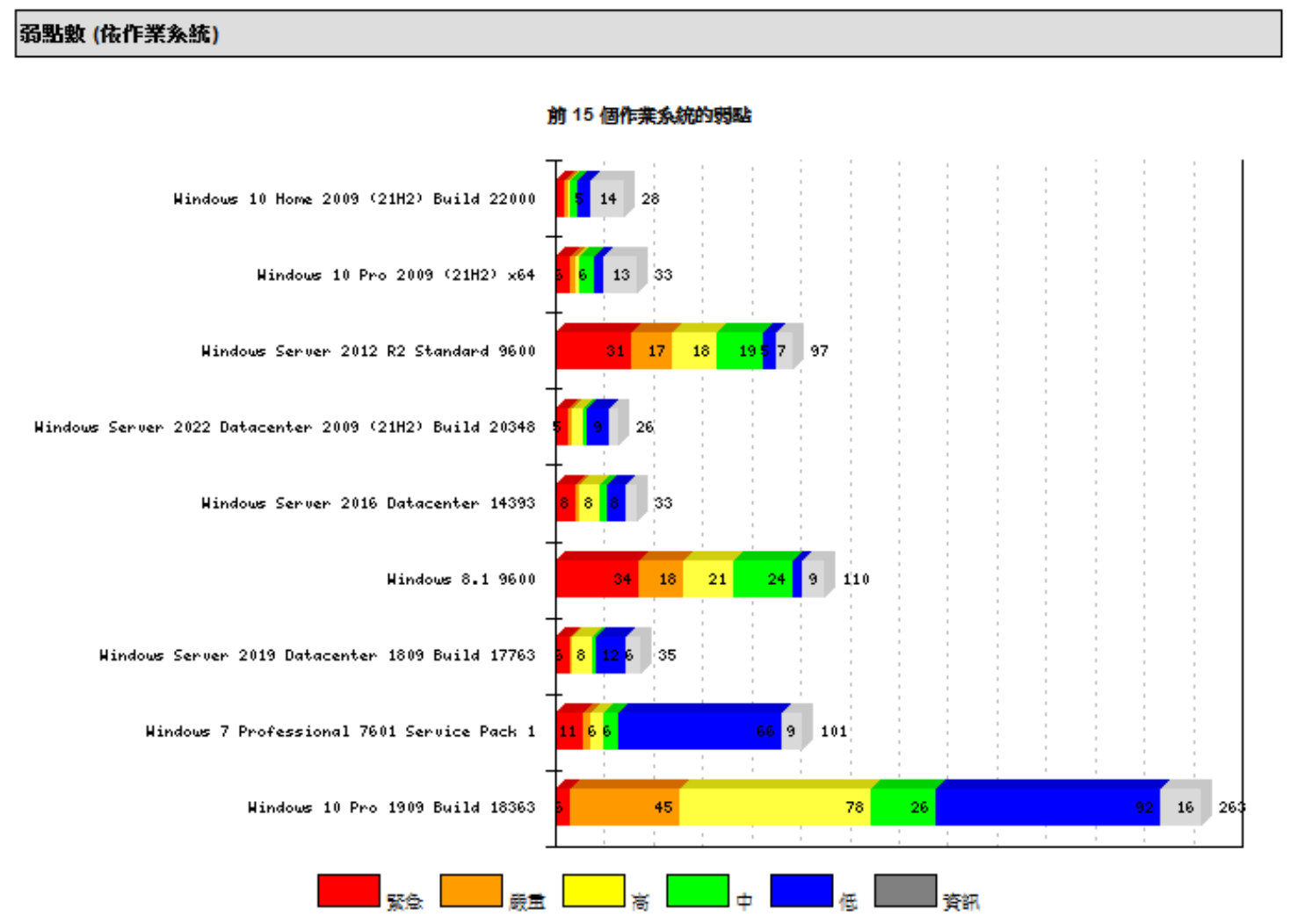
vm-win81	[TCP - 445] Native OS: Windows 8.1 9600 Native LAN Manager: Windows 8.1 6.3	192.168.1.19
WIN-TGSK9K74R18	[TCP - 445] Native OS: Windows Server 2016 Datacenter 14393 Native LAN Manager: Windows Server 2016 Datacenter 6.3	192.168.1.48
WIN7-Clean-新	[UDP - 137] MAC Address: 00-0C-29-14-D7-F7 NIC Vendor: VMware, Inc. Name Table: WIN7-CLEAN-s <0><UNIQUE>@13 HOME <0><GROUP>@13 HOME <1E><GROUP>@13 WIN7-CLEAN-s <20><UNIQUE>@13 Probe Hex: \x04\x80\xF0\x84\x00\x00\x00\x00\x01\x00\x00\x00\x00\x20\x43\x4B@13 \x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41@13 \x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x00\x00@13 \x21\x00\x01\x00\x00\x00\x00\x00\x77\x04\x57\x49\x4E\x37\x2D\x43@13 \x4C\x45\x41\x4E\x2D\xB7\x73\x20\x20\x00\x04\x00\x48\x4F\x4D\x45@13 \x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x00\x84\x00\x48\x4F@13 \x4D\x45\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x1E\x84\x00@13 \x57\x49\x4E\x37\x2D\x43\x4C\x45\x41\x4E\x2D\xB7\x73\x20\x20\x20@13 \x04\x00\x00\x0C\x29\x14\xD7\xF7\x00\x00\x00\x00\x00\x00\x00\x00@13 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00@13 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 Probe Text: ..... CKAAAAAAAAAAAAAAAAAAAAAAAAAAAA..!.....w.WIN7-CLEAN-.s ...HOME ...HOME ...WIN7-CLEAN-.s ....).....	192.168.1.12

管理報告包含整體統計

弱點(依風險)

風險等級	弱點名稱 VID	偵測到的主機	受影響的系統	易受攻擊的執行個體
緊急	密碼長度最小值太短或未設定 [VID 12]	10	WIN7-Clean-新, 192.168.1.12	1
			win10-1903, 192.168.1.15	1
			vm-win81, 192.168.1.19	1
			WIN7-x64pro, 192.168.1.24	1
			WIN-S-2022, 192.168.1.32	1
			DESKTOP-61EQU0D, 192.168.1.43	2
			WIN-TGSK9K74R18, 192.168.1.48	1
			ASUS-Win11, 192.168.1.89	1
			WIN-490L315DHB3.localdomain, 192.168.21.128	1
緊急	密碼最長使用期限太短 [VID 14]	4	WIN7-Clean-新, 192.168.1.12	1
			vm-win81, 192.168.1.19	1
			WIN7-x64pro, 192.168.1.24	1
			WIN-490L315DHB3.localdomain, 192.168.21.128	1
緊急	密碼不會過期 [VID 15]	9	win10-1903, 192.168.1.15	1
			vm-win81, 192.168.1.19	1
			WIN7-x64pro, 192.168.1.24	1
			WIN-S-2022, 192.168.1.32	1
			DESKTOP-61EQU0D, 192.168.1.43	2

管理報告包含整體統計


弱點數 (依作業系統)
前 15 個作業系統的弱點
Windows 10 Home 2009 (21H2) Build 22000
Windows 10 Pro 2009 (21H2) x64
Windows Server 2012 R2 Standard 9600
Windows Server 2022 Datacenter 2009 (21H2) Build 20348
Windows Server 2016 Datacenter 14393
Windows 8.1 9600
Windows Server 2019 Datacenter 1809 Build 17763
Windows 7 Professional 7601 Service Pack 1
Windows 10 Pro 1909 Build 18363
28
33
97
26
33
110
35
101
263
緊急
嚴重
高
中
低
資訊

管理報告包含整體統計

弱點(依作業系統)

作業系統	緊急	嚴重	高	中	低	資訊
Windows 10 Pro 1909 Build 18363	6	45	78	26	92	16
Windows 7 Professional 7601 Service Pack 1	11	3	6	6	66	9
Windows Server 2019 Datacenter 1809 Build 17763	6	1	8	2	12	6
Windows 8.1 9600	34	18	21	24	4	9
Windows Server 2016 Datacenter 14393	8	2	8	3	8	4
Windows Server 2022 Datacenter 2009 (21H2) Build 20348	5	2	4	2	9	4
Windows Server 2012 R2 Standard 9600	31	17	18	19	5	7
Windows 10 Pro 2009 (21H2) x64	6	2	2	6	4	13
Windows 10 Home 2009 (21H2) Build 22000	4	1	1	3	5	14

管理報告包含整體統計

MS17-022:Microsoft XML Core Services 的安全性更新 (4010321) [VID 6608] CVSS 9.3 (緊急)

說明

此安全性更新可解決 Microsoft Windows 中的弱點。如果使用者造訪蓄意製作的網站，此弱點可能會允許資訊洩漏。但是，無論如何，攻擊者無法強迫使用者按一下蓄意製作的連結。攻擊者必須引誘使用者按一下連結，一般是藉助電子郵件的附件或 Instant Messenger 訊息。此更新會變更 MSXML 處理記憶體中物件的方式，藉此解決弱點。

詳細資訊請參閱：

MS17-022

https://technet.microsoft.com/library/security/MS17-022

Microsoft Security Bulletin Summary for March 2017

https://technet.microsoft.com/library/security/ms17-mar.aspx

連線

執行 Windows 更新和修補，或從下面的連結下載更新

http://technet.microsoft.com/security/bulletin/MS17-022

一般弱點及揭露 (CVE) 連結:

CVE-2017-0022

受影響的系統

系統	作業系統
vm-win81, 192.168.1.19	Windows 8.1 9600
WIN-TGSK9K74R18, 192.168.1.48	Windows Server 2016 Datacenter 14393

單主機
弱點掃描報告
HTML/PDF 格式

單主機報表 – 統計圖表

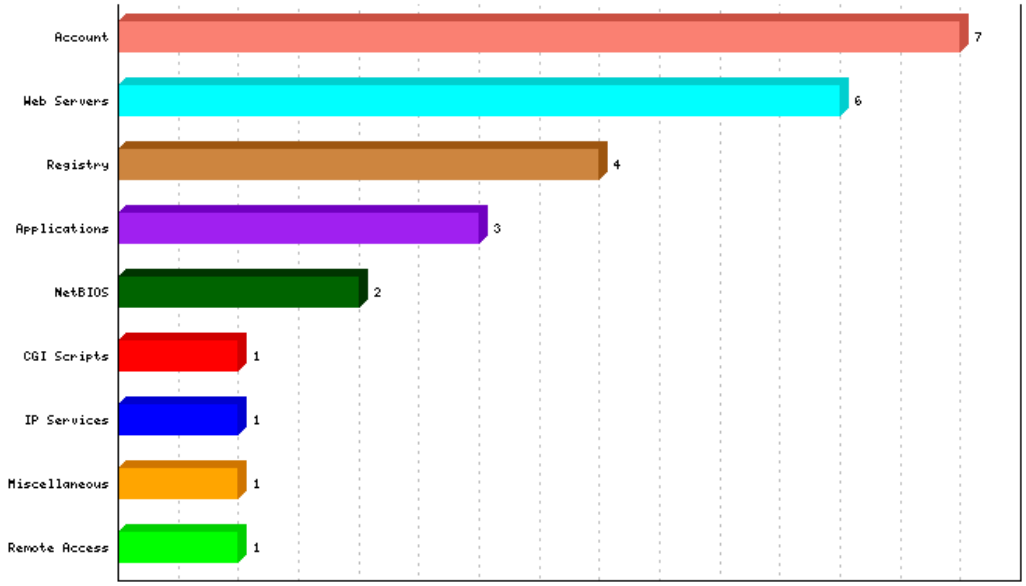
HTML 報表 | PDF 報表 | 報表選項: 統計圖表 | 通訊埠 | Windows 帳號 | Windows 服務 | 軟體資產 | 網芳分享 | 工作檢核表

4MOSAn Vulnerability Management

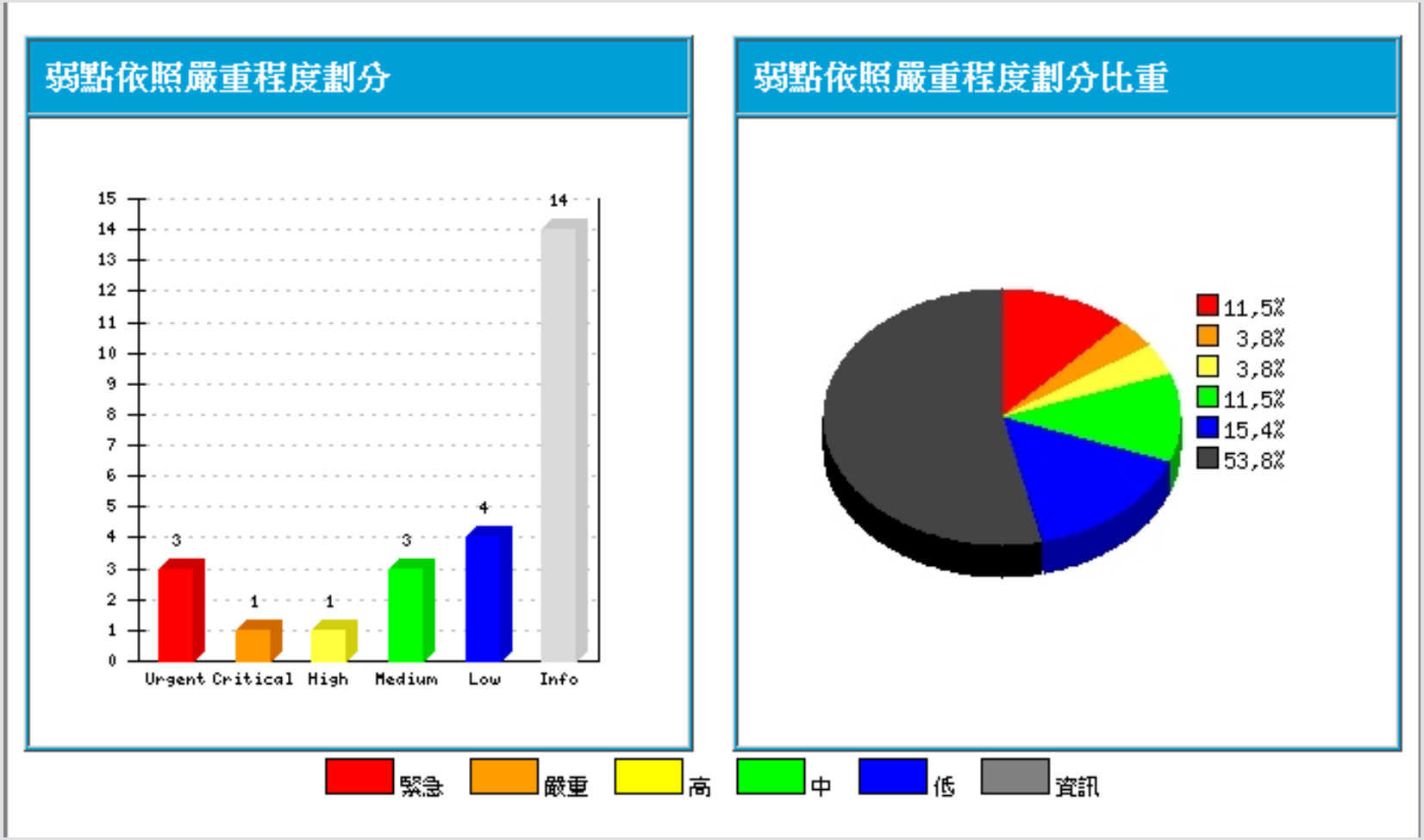
掃描規範

開始時間: 2022/08/22 12:39:11
弱點評估版本: 4.2.3.0 (2022-06-08)
結束時間: 2022/08/22 12:44:47
弱點更新日期: 2022-08-10
耗費時間: 00:05:36
報表產生: 2022/09/30 GMT 8

稽核類型分佈統計圖



單主機報表 – 統計圖表


弱點依照嚴重程度劃分
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
0
3
1
1
3
4
14
Urgent
Critical
High
Medium
Low
Info
弱點依照嚴重程度劃分比重
11,5%
3,8%
3,8%
11,5%
15,4%
53,8%
緊急
嚴重
高
中
低
資訊

單主機報表 – 技術性報表

- 弱點名稱與內容描述
1. 弱點嚴重性等級 (緊急、嚴重、高、中、低)
2. 弱點修補建議
3. 弱點影響 (C)機密性 (I)完整性 (A)可用性
4. 弱點 CVSS v2 基本評分
5. 弱點 CVE 編號
6. 弱點判斷的依據
7. 弱點參考資料
- 網路服務(通訊埠)開啟列表及資訊
- Windows 帳號、分享、服務、軟體資產列表

單主機報表 – 技術性報表

192.168.1.89 : ASUS-Win11

開始時間: 2022/08/22 12:39:11 - 2022/08/22 12:44:47
IP 位址: 192.168.1.89
電腦名稱: ASUS-WIN11
工作群組: HOME
作業系統: Windows 10 Home 2009 (21H2) x64
Windows 版本: Windows (Version 10.0, Build 0, 64-bit Edition)
系統安裝日期: 2021-12-23 7:31:4
IE 版本: IE9, Update:11.0.1000 (), Version:11.1.22000.0
防毒軟體名稱: Windows Defender Up to date (Enabled)
主機板生產商: ASUSTeK COMPUTER INC.
主機板型號: D700TC
BIOS 版本: _ASUS_ - 1072009 D700TC.311 American Megatrends - 50013
CPU 規格: 11th Gen Intel(R) Core(TM) i7-11700 @ 2.50GHz
RAM 規格: 16 GBytes
MAC 供應商: ASUSTek COMPUTER INC.
MAC / 閘道: 04-42-1A-8E-39-3E
磁碟: C 磁碟, 磁碟容量: 475.69GB, 剩餘: 394.06GB (83 %)
磁碟: D 磁碟, 磁碟容量: 488.28GB, 剩餘: 128.13GB (26 %)
磁碟: E 磁碟, 磁碟容量: 488.28GB, 剩餘: 440.38GB (90 %)
磁碟: F 磁碟, 磁碟容量: 488.28GB, 剩餘: 201.61GB (41 %)
磁碟: G 磁碟, 磁碟容量: 398.16GB, 剩餘: 381.23GB (96 %)

嚴重性層級:  (緊急)

單主機報表 – 技術性報表

稽核

[例外] 密碼歷程紀錄未強制執行		嚴重性: (緊急)
內容描述:	這項原則設定使用新密碼之前, 必須與使用者帳戶之前用過舊密碼不能重複的數目. 這個值必須介於 0 至 24 個密碼之間. 這項原則可讓系統管理員藉由確定使用者不再重複使用舊密碼, 以增加安全性.	
修補建議:	1. 打開 [控制台\系統管理工具\本機安全性原則\安全性設定\帳戶原則\密碼原則\強制執行密碼歷程記錄] 2. 輸入記憶的密碼組數 (建議 4 組以上. GCB 設定值為 3).	
影響:	(C)機密性: 全部, (I)完整性: 全部, (A)可用性: 全部	
CVSS v2 基本評分:	7 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	CVE 編號: CVE-1999-0535
參考資料:	. CCE-8912-8 http://cce.mitre.org	
例外說明:	不管它	
密碼歷程紀錄未強制執行 Response: 0		

密碼長度最小值太短或未設定		嚴重性: (緊急)
內容描述:	此項安全性設定使用者帳戶的密碼必須包含的最少字元數. 可以設定介於 1 至 14 個字元之間的值. 如果字元數設為 0 則表示不需要密碼.	
修補建議:	1. 打開 [控制台\系統管理工具\本機安全性原則\安全性設定\帳戶原則\密碼原則\最小密碼長度] 2. 輸入最大天數 (建議為 8 個字元或以上).	
影響:	(C)機密性: 全部, (I)完整性: 全部, (A)可用性: 全部	
CVSS v2 基本評分:	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	CVE 編號: CVE-1999-0535
參考資料:	. CCE-9357-5 http://cce.mitre.org . CCE-2981-9 http://cce.mitre.org	
密碼長度最小值太短或未設定 Response: 0		

單主機報表 – 技術性報表

MS20-Aug:CVE-2020-1472-Zerologon 弱點		嚴重性: (高)
內容描述:	Windows 重大漏洞 Zerologon 可讓駭客輕易掌控 AD 網域, 遠端攻擊者只需對有漏洞的 DC 建立 TCP 連線, 無需任何網域登入的帳號與密碼便可以獲得 AD 管理員權限, 控制整個 Windows 網域, 包括在網域上任何主機上執行惡意應用程式. 此安全性更新可解決 Microsoft Windows 中的弱點.	
修補建議:	執行 Windows 更新和修補，或從下面的連結下載更新 https://portal.msrc.microsoft.com/security-guidance/advisory/CVE-2020-1472	
影響:	(C)機密性: 全部, (I)完整性: 全部, (A)可用性: 全部	
CVSS v2 基本評分:	7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)	CVE 編號: CVE-2020-1472
參考資料:	. CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability https://portal.msrc.microsoft.com/security-guidance/advisory/CVE-2020-1472 . Security update deployment information: September 8 2020 https://support.microsoft.com/help/20200908/ . SecuraBV / CVE-2020-1472 https://github.com/SecuraBV/CVE-2020-1472 . risksense / zerologon https://github.com/risksense/zerologon	
HotFix: KB4565349		

KB4535680：x64 系統的 Windows Server 2019 安全性更新		嚴重性: (高)
內容描述:	現在已經證實 Microsoft 軟體產品中有一個安全性問題, 可能會影響您的系統. 您可以安裝此 Microsoft 更新來保護您的系統. 如需此更新包含的完整問題清單, 請參閱相關的 Microsoft 知識庫文章. 安裝此更新後, 您可能必須重新啟動系統. 2021-01-12	
修補建議:	Microsoft Update Catalog: https://www.catalog.update.microsoft.com/Search.aspx?q=KB4535680	
CVSS v2 基本評分:	6	CVE 編號:
參考資料:	. KB4535680 http://support.microsoft.com	

單主機報表 – 技術性報表

通訊埠

Num	內容描述	稽核	風險	Banner
135	Microsoft Remote Procedure Call (RPC) service	14	緊急	
139	NETBIOS Session Service	0		
445	Microsoft-DS	0		
1900	SSDP	0		

分享

名稱	內容描述	密碼
ADMIN$	遠端管理	無
C$	預設共用	無
IPC$	遠端 IPC	
Users		無
新增資料夾		無

服務

名稱	內容描述	狀態	啟動類型
wuauserv	Windows Update	已啟動	手動
WSearch	Windows Search		停用
WpnService	Windows 推播通知系統服務	已啟動	自動
WPDBusEnum	Portable Device Enumerator Service	已啟動	手動
WMPNetworkSvc	Windows Media Player Network Sharing Service		手動

單主機報表 – 技術性報表

軟體資產

內容描述
Google Chrome
4MOSAn 政府組態基準設定與檢測 4.1
4MOSAn 分散式弱點管理 4.0

帳號

名稱	密碼	權限	註解
WDAGUtilityAccount		Guest	系統針對 Windows Defender 應用程式防護案例所管理及使用的使用者帳戶。
Guest		Guest	供來賓存取電腦/網域之用的內建帳戶
DefaultAccount		Guest	由系統管理的使用者帳戶。
Administrator		Administrator	管理電腦/網域的內建帳戶

弱點管理工作檢核表

填表日期: 年 月 日

IP 位址: 192.168.1.43	**主機名稱:** WIN-2019-Data	**作業系統:** Windows Server 2019 Datacenter 1809 x64
掃描時間: 2022/10/01	**管理人員:**	**用途:**

序號	風險	弱點名稱	處理情形	處理日期	無法修補 原因說明
1	緊急	密碼長度最小值太短或未設定	□待修補□已修補 □無法修補		
2	緊急	密碼不會過期	□待修補□已修補 □無法修補		

工作檢核表

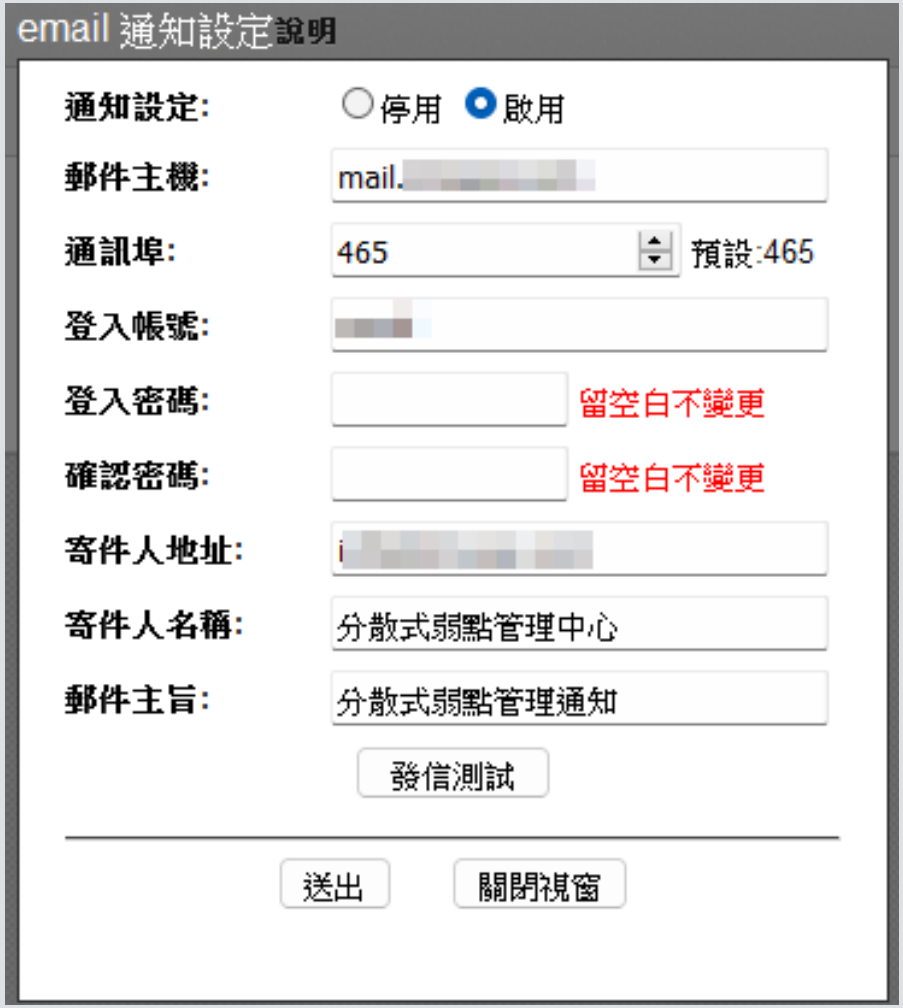
弱點管理工作檢核表

填表日期: 年 月 日

IP 位址: 192.168.1.89	**主機名稱:** ASUS-Win11	**作業系統:** Windows 10 Home 2009 (21H2) x64
掃描時間: 2022/08/22	**管理人員:**	**用途:**

序號	風險	弱點名稱	處理情形	處理日期	無法修補 原因說明
1	緊急	密碼長度最小值太短或未設定	□待修補□已修補 □無法修補		
2	緊急	密碼不會過期	□待修補□已修補 □無法修補		
3	緊急	密碼超過最長有效期	□待修補□已修補 □無法修補		
4	嚴重	測試 HTTP 危險方法	□待修補□已修補 □無法修補		
5	高	帳戶鎖定閾值	□待修補□已修補 □無法修補		
6	中	印表機驅動程式安全	□待修補□已修補 □無法修補		
7	中	未登入關機啟用	□待修補□已修補 □無法修補		
8	中	Apache HTTP Server 2.4.51 之前版本多個弱點	□待修補□已修補 □無法修補		

Email 設定


email 通知設定說明
通知設定:
停用
啟用
郵件主機:
mail.
通訊埠:
465
預設:465
登入帳號:
登入密碼:
留空白不變更
確認密碼:
留空白不變更
寄件人地址:
寄件人名稱:
分散式弱點管理中心
郵件主旨:
分散式弱點管理通知
發信測試
送出
關閉視窗

Email 通知

寄件者: 分散式弱點管理中心 <[redacted]>
收件者: [redacted]
副本:
主旨: 分散式弱點管理通知

分散式弱點管理檢測完成通知

檢測單位: [redacted]
檢測主機: VM-WIN81
檢測時間: 2022-09-30 20:49:27
檢測間隔: 91 天
下次檢測: 2022-12-30 20:49:00
查看最新的檢測報告:
https://[redacted]n=ba675d

本郵件由 4MOSAn 分散式弱點管理中心寄出.

Email 通知

- 弱點檢測後發出通知信件給電腦列表中, 主機使用者的 E-mail
- 新增帳號、刪除帳號之後, 寄送郵件通知給相關帳號的 E-mail
- 帳號之密碼變更之後, 寄送郵件通知給相關帳號設定的 E-mail
- 設定派送軟體之後, 寄送郵件通知給全部系統管理員以及全部單位管理員的 E-mail

4MOSAn 美麗島安全科技

點選連結檢視報告

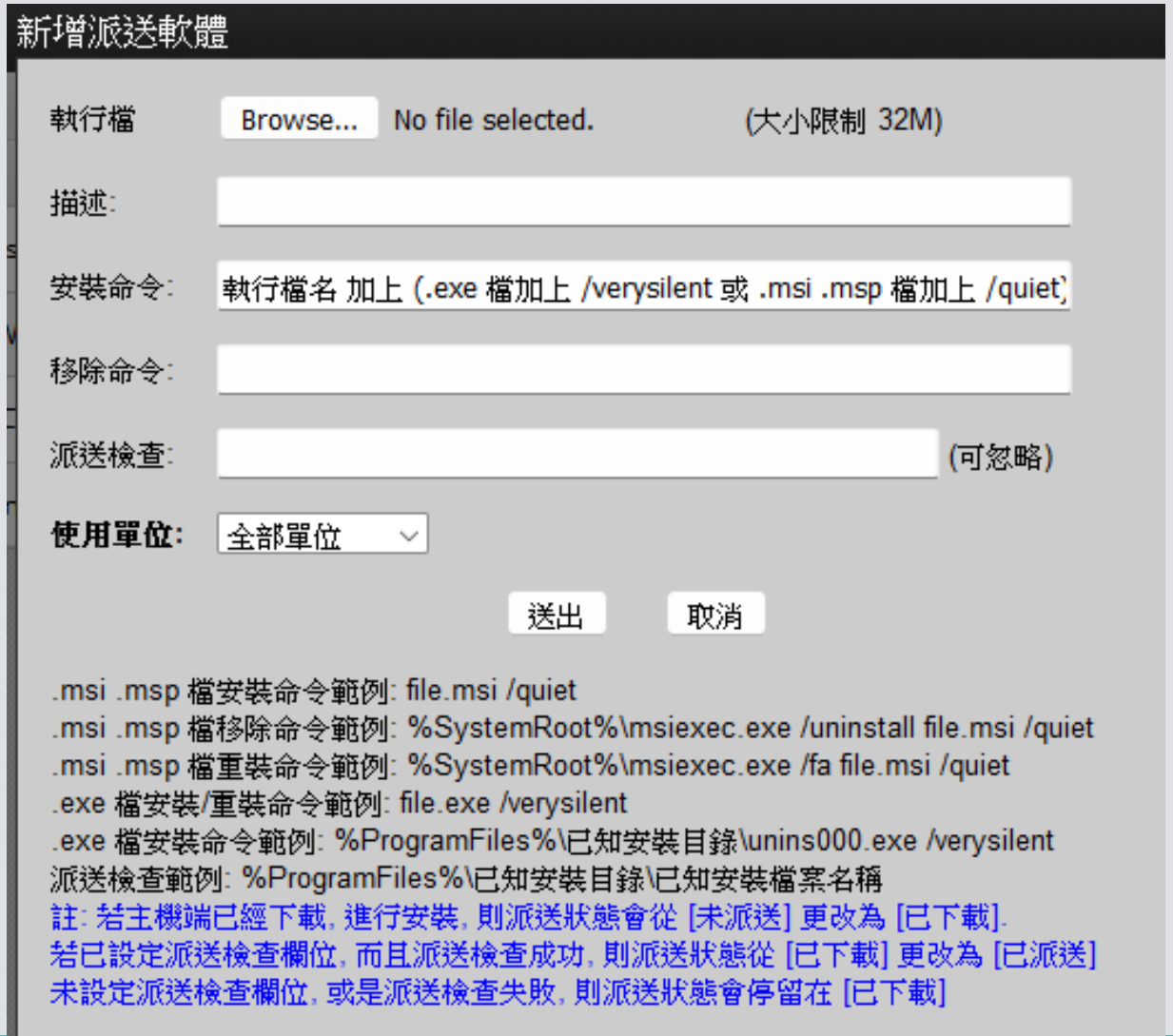
Num	嚴重性	CVSS	弱點名稱	弱點類型
1	緊急	7	密碼歷程紀錄未強制執行 [例外]	Account
2	緊急	10	密碼長度最小值太短或未設定	Account
3	緊急	10	密碼最長使用期限太短	Account
4	緊急	10	密碼不會過期	Account
5	緊急	10	不限制存取光碟	Registry
6	緊急	10	不限制存取軟碟	Registry
7	緊急	9.3	MS14-074:遠端桌面通訊協定中的資訊安全風險可能會允許略過資訊安全功能 (3003743)	Windows Hotfix
8	緊急	9.3	MS15-034:HTTP.sys 中的資訊安全風險可能會允許遠端執行程式碼 (3042553)	Windows Hotfix
9	緊急	9.3	MS15-060:Microsoft 通用控制項中的弱點可能會允許遠端執行程式碼 (3059317)	Windows Hotfix
10	緊急	9.3	MS15-075:OLE 中的資訊安全風險可能會允許提高權限 (3072633)	Windows Hotfix
11	緊急	9.3	MS15-082:RDP 中的弱點會允許遠端程式碼執行 (3080348)	Windows Hotfix
12	緊急	9.3	MS16-027:用來解決遠端執行程式碼的 Windows Media 安全性更新 (3143146)	Windows Hotfix
13	緊急	9.3	MS16-032:用來解決權限提高的 Secondary Logon 安全性更新 (3143141)	Windows Hotfix
14	緊急	9.3	MS16-047:SAM 和 LSAD 遠端通訊協定的安全性更新 (3148527)	Windows Hotfix

軟體派送功能

- 軟體派送功能具備密碼保護
- 允許派送 msi、exe、msp (Windows Installer Patch)

- 軟體派送紀錄: 保留一年內的紀錄
- 派送功能包括: [安裝、移除] 軟體
- 可篩選作業系統作業系統，搜尋特定弱點，
  大量派送 . msp (Windows Installer Patch) 或
  其他軟體版本升級 (如 Java SE、Acrobat Reader)

軟體派送


新增派送軟體
執行檔
Browse...
No file selected.
(大小限制 32M)
描述:
安裝命令:
執行檔名 加上 (.exe 檔加上 /verysilent 或 .msi .msp 檔加上 /quiet)
移除命令:
派送檢查:
(可忽略)
使用單位:
全部單位
送出
取消
.msi .msp 檔安裝命令範例: file.msi /quiet
.msi .msp 檔移除命令範例: %SystemRoot%\msiexec.exe /uninstall file.msi /quiet
.msi .msp 檔重裝命令範例: %SystemRoot%\msiexec.exe /fa file.msi /quiet
.exe 檔安裝/重裝命令範例: file.exe /verysilent
.exe 檔安裝命令範例: %ProgramFiles%\已知安裝目錄\unins000.exe /verysilent
派送檢查範例: %ProgramFiles%\已知安裝目錄\已知安裝檔案名稱
註: 若主機端已經下載, 進行安裝, 則派送狀態會從 [未派送] 更改為 [已下載].
若已設定派送檢查欄位, 而且派送檢查成功, 則派送狀態從 [已下載] 更改為 [已派送]
未設定派送檢查欄位, 或是派送檢查失敗, 則派送狀態會停留在 [已下載]

密碼政策與帳戶政策

- 最小密碼長度 (可自訂)
- 符合複雜性需求 (可自訂)
- 允許密碼重複使用 (可自訂)
- 密碼使用期限: (天數可自訂)

- 帳戶鎖定閾值: 5 次
- 重設帳戶鎖定計數器的時間: 15 分鐘
- 帳戶鎖定期間 (帳戶鎖定時間): 15 分鐘

- 可限制登入 IP 位址
- 登入紀錄: 保留一年內的紀錄

支援雙重驗證 (Google Authenticator)

分散式弱點管理

- 彌補傳統式網路型弱點掃描的局限
- 檢測過程不佔用頻寬，不影響網路設備與流量
- 檢測結果準確，可以避免網路因素造成誤判
- 降低人力、交通、住宿、時間等成本
  (只需到場一次進行安裝，或由用戶自行安裝)

- 有如戰情指揮中心般的弱點管理系統