TWCERT/CC 資安情資電子報

2024 年 7 月份

電子報序言

台灣電腦網路危機處理暨協調中心(以下簡稱 TWCERT/CC)在數位發展部指導下，推動企業資安通報協處、產品資安漏洞通報、惡意檔案檢測服務及資安情資分享等工作，以提升國家資安聯防能量，並維護整體網路安全。

TWCERT/CC 本月份所發布之資安情資電子報，為透過官方網站、電子郵件及電話等方式接收資安情資，並與國內外 CERT/CSIRT、資安組 織、學研機構、民間社群、政府單位及私人企業間資安情資共享，將接收與共享之情資進行彙整、分析與分享，主要分成以下 4 章節：

第1章、封面故事：本月TWCERT/CC所發布之資安情資中，官網點閱次數最高之情資列為本月份封面故事。

第2章、國內外重要資安事件：研析國內外相關資安情報，及彙整上述方式接收之資安情資，進行分析與分享。範疇可能包含資訊安全宣導、資安趨勢、國際政府組織資安資訊、社群媒體資安近況、行動裝置資安訊息、軟硬體系統資安議題、軟硬體漏洞資訊及新興應用資安。

第3章、資安研討會及活動：近期舉辦之國內外資安相關研討會、訓練課程及資安競賽等活動資訊分享。

第4章、TVN漏洞公告：TWCERT/CC為CVE編號管理者 (CVE Numbering Authorities, CNA)，協助國內外廠商處理產品漏洞並完成漏洞修補，此章說明本月發布於台灣漏洞揭露 (Taiwan Vulnerability Note, TVN)平台其CVSS 3分數為8.8以上之漏洞。

目錄

內容

目錄 II

第 1 章、封面故事 1

OpenSSH 問世以來第一個 RCE: CVE-2024-6387 1

第 2 章、國內外重要資安事件 4

2.1 新興應用資安 4

2.1.1 新型態的工控攻擊逐漸成為主流：以 PLC 作為惡意中繼站 4

2.2 資安趨勢 8

2.2.1 基於 Golang 的勒索軟體 Eldorado，可跨平台攻擊 8

2.3 軟硬體系統資安議題 11

2.3.1 GeoServer 漏洞曝光：開源地理位置資訊伺服器受到攻擊風險 11

2.3.2 大量Windows出現藍色當機畫面，資安公司CrowdStrike緊急修補更新程式 14

2.4 資訊安全宣導 18

2.4.1 AI軟體與服務可能產生之風險疑慮 18

2.5 軟硬體漏洞資訊 20

2.5.1 Linux kernel存在高風險安全漏洞 20

2.5.2 OpenSSH存在高風險安全漏洞 22

2.5.3 GeoServer存在高風險安全漏洞 23

2.5.4 GeoServer之開源專案JAI-EXT存在高風險安全漏洞 24

2.5.5 Microsoft Windows MSHTML Platform存在高風險安全漏洞 25

2.5.6 Cisco 思科郵件安全閘道(Secure Email Gateway)存在高風險安全漏洞 27

2.5.7 Cisco 思科SSM On-Prem存在高風險安全漏洞 28

第 3 章、資安研討會及活動 29

第 4 章、TVN 漏洞公告 36

編輯：TWCERT/CC 團隊 40

第 1 章、封面故事

OpenSSH 問世以來第一個 RCE: CVE-2024-6387

OpenSSH 從1995 年問世以來，這是第一次出現遠端執行任意程式碼(RCE)漏洞(regreSSHion)，可以用最高管理員權限來遠端執行指令對系統控制，研究人員將它稱為regreSSHion。

OpenSSH 是一個基於 SSH 協定的開源軟體，常見於 Linux 中使用，作為遠端登入系統管理，也可進行遠端檔案傳輸，此次漏洞在 2024 年 5 月被資安公司 Qualys 發現並將其命為regreSSHion(漏洞編號：CVE-2024-6387)，漏洞問題出現在檔案 sshd中，可以讓未經授權的攻擊者以 root 身分執行任意程式。

sshd 是 OpenSSH Server 的設定檔案，其存在一個變數

LoginGraceTime ，若沒有更改這個變數值，預設是 120 秒，它是代表給予使用者進行身分驗證的時間，所以當使用者使用 ssh 連接時，超過 LoginGraceTime 設定的時間 (預設 120 秒) 沒有完成身分驗證，則 sshd 會去呼叫 SIGALRM 信號處理，並會呼叫不安全的非同步函數做處理，而攻擊者可以在此時利用競爭情況(race condition) 以最高管理員權限執行任意程式碼。

競爭情況 (race condition) 常見於多執行緒的系統，當多個執行緒同時存取或修改共享的資料時就會發生這個問題。

在 sshd 處理 SIGALRM 信號時，就有可能觸發競爭情況，而這就可能導致未預期的行為。

經過研究人員的調查，此漏洞實際上是CVE-2006-5051 的回歸，CVE-2006-5051 是在 2006 年由 Mark Dowd 發現，他跟此次漏洞一樣都是信號處理競爭情況的漏洞，可以讓攻擊者造成阻斷服務攻擊。

稱之為回歸是因為在 2020 年 10 月 OpenSSH 版本 8.5p1 的更新 (commit 編號：752250c)，把 OpenSSH 裡面 sshd 程式的 SIGALRM 信號處理函數 sigdie() ，刪除其中一行程式碼 #ifdef DO_LOG_SAFE_IN_SIGHAND，而這也造成了：

- OpenSSH 版本小於 4.4p1 會遭受漏洞影響，這是對 CVE-2006-5051 的錯誤修補
- 4.4p1 <= OpenSSH 版本 < 8.5p1 並無受此漏洞影響，因為 CVE-2006-5051 有添加 #ifdef DO_LOG_SAFE_IN_SIGHAND
- 8.5p1 <= OpenSSH 版本 < 9.8p1 再次容易受到威脅影響，因為 #ifdef DO_LOG_SAFE_IN_SIGHAND 意外被刪除了

Qualys 研究人員指出雖然漏洞影響很大，但要實際攻擊成功並不容易，在他們的測試實驗上，平均測試連線 1 萬次才成功一次做

到攻擊。

研究人員用兩個不同的作業系統做測試，以 ubuntu-6.06.1-server-i386.iso 這個 Ubuntu 版本測試，平均成功攻擊一次約需要 1 ~ 2 天，而用 debian-12.5.0-i386-DVD-1.iso (這是目前 Debian 穩定版)，平均攻擊成功一次約需要 6 ~ 8 小時。

目前研究人員透過 Shodan 和 Censys 對全世界網路進行掃描，有超過 1400 萬台的 OpenSSH Server 暴露在網路上。

而 Qualys 研究人員表示裡面存在 70 萬個 OpenSSH Server 處在易受攻擊的狀態。

受影響的軟體版本：

- OpenSSH 版本 < 4.4p1
- 8.5p1 <= OpenSSH版本 < 9.8p1

為了避免被攻擊，建議使用者：

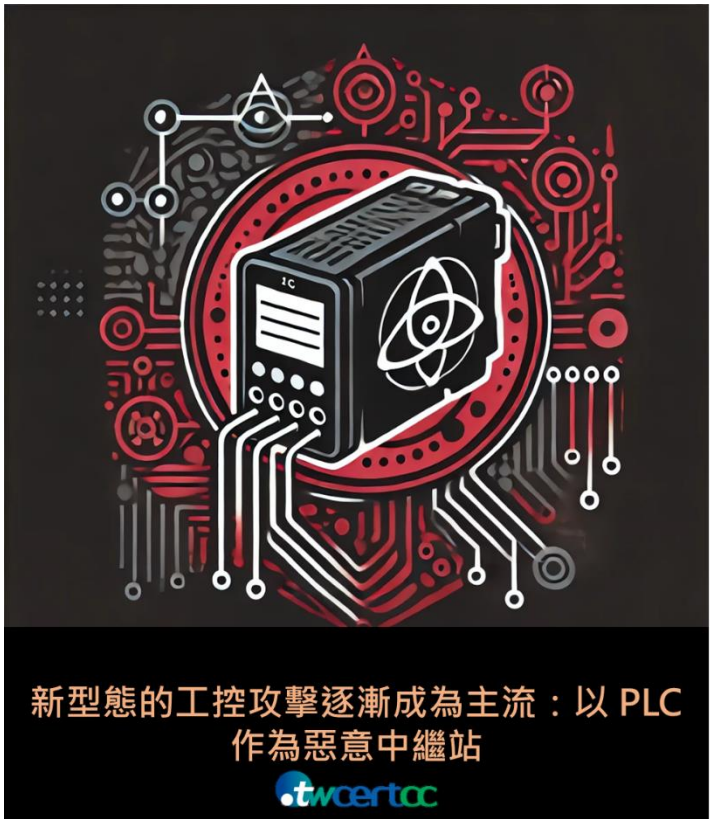
- 升級 OpenSSH 到最新的版本 9.8p1 來修復此漏洞
- 如果暫時不能更新 OpenSSH ，則可以更改 sshd 的變數 LoginGraceTime ，將其設定為 0 ，惟可能會遭受阻斷服務攻擊

- 資料來源：
  1. regreSSHion: RCE in OpenSSH's server, on glibc-based Linux systems (CVE-2024-6387)

第 2 章、國內外重要資安事件

2.1 新興應用資安

2.1.1 新型態的工控攻擊逐漸成為主流：以 PLC 作為惡意中繼站



2024年7月8日俄羅斯資安公司 Solar 的網路威脅情資中心(4RAYS)資安人員揭露一個親烏克蘭APT 組織：Lifting Zmiy 對俄羅斯政府和私人公司進行一系列的攻擊活動。

攻擊活動追蹤時間為 2023 年 9 月至 2024 年 6 月發生的4 起攻擊事件作分析，目標為俄羅斯工控自動化公司Tekon-Avtomatika 的可程式化邏輯控制器(Programmable Logic Controller，PLC) 設備，型號為 KUN-IP8，並在設備上部署中繼站，進而以此攻擊其他目標，研究人員分析發現受害者遍及各個行業，Linux 和 Windows 系統均無

法幸免。

此次威脅研究足以表明，過往大多認為營運科技(Operation Technology, OT)網路攻擊是透過入侵資訊科技(Informatiom Technology, IT)系統做為跳板，進而滲透至OT環境，而本次的攻擊則是先透過入侵OT環境後，轉攻擊IT。此次問題的原因在於PLC設備使用了預設的憑證資訊。

資安人員Jose Bertin 在2022年3月研究指出存在大量使用預設最高管理員憑證的PLC設備，而這些憑證資訊當時公開在 Tekon-Avtomatika 公司的官方網站上，儘管該公司隨後即刪除預設最高管理員憑證，但仍有不少設備並未更改，而APT組織 Lifting Zmiy 即利用這些資訊入侵PLC設備，並將其作為中繼站。此外，這些中繼站IP的供應商為 Starlink Services LLC ，其為SpaceX的一個部門，SpaceX在全世界各地提供衛星網路服務，駭客透過SpaceX的 Starlink 基礎設施來隱蔽其行蹤，且受益於動態IP，以規避物理位置的檢測分析，為駭客提供一個難以被追蹤和監控的攻擊平台。

然而，在此之前已有資安人員對OT環境安全感到憂心，BlackHat USA 2015 演講：INTERNET-FACING PLCS-A NEW BACK ORIFICE 和BlackHat Asia 2016演講：PLC-Blaster:A Worm Living Solely in the PLC共同探討透過感染 PLC 作為中繼站的展示，此次研究是歷史上首個公開研究針對攻擊 PLC 作為 中繼站跳板的攻擊，研究人員寫了一個概念性驗證程式，給其名字為：PLC-Blaster，他是研究人員為了測試而開發的概念性驗證的蠕蟲(一種惡意程式類型)。攻擊對像為西門子所開發的PLC設備，型號為 S7-1200，研究人員是透過將惡意程式寫入至PLC，使PLC作為跳板執行命令作攻擊行為。

此次研究站在防禦的角度上，過往工控資安防禦主要為對HMI和PLC之間的流量建立Baseline來偵測異常，並實施白名單管制，從Purdue Model角度來看，關注的安全防護主要是垂直的。垂直的意思

是HMI和PLC之間的通訊，也就是Purdue Model裡面Level 2 和Level 1之間的網路流量，而鮮少探討水平之間的流量檢測，水平的意思就是Purdue Model裡面Level 1和Level 1之間的通訊流量，且過往白名單會去信任PLC，所以透過PLC發出的流量會無條件被信賴，此次研究則利用此問題，透過控制 PLC 作為跳板進行攻擊以規避防禦產品偵測。

近期2022 年由工控資安公司Claroty的Team82 研究團隊曾發布白皮書：EVIL PLC ATTACK: WEAPONIZING PLCS，內容研究的攻擊名字取名為：Evil PLC，主要是透過感染 PLC 讓其武器化可以執行命令。

研究人員撰寫了概念性驗證程式並對 7 家工控廠商(洛克威爾公司、施耐德電氣公司、通用電氣公司、貝加萊公司、信捷電氣公司、英國奧威公司、艾默生電氣公司)的PLC設備進行測試，顯示過往PLC多為攻擊的目標，如歷史出現過的資安事件：Stuxnet,Incontroller/Pipedream等，但此研究是將 PLC作為攻擊使用的武器，來進一步對其他系統作攻擊，雖然非真實的案件，但也證明這樣的攻擊情境是值得關注的。

總結來說，過往針對工控的安全大多會無條件去信任PLC，且一般已知攻擊主要都是透過感染IT系統之後擴散攻擊至OT 環境。

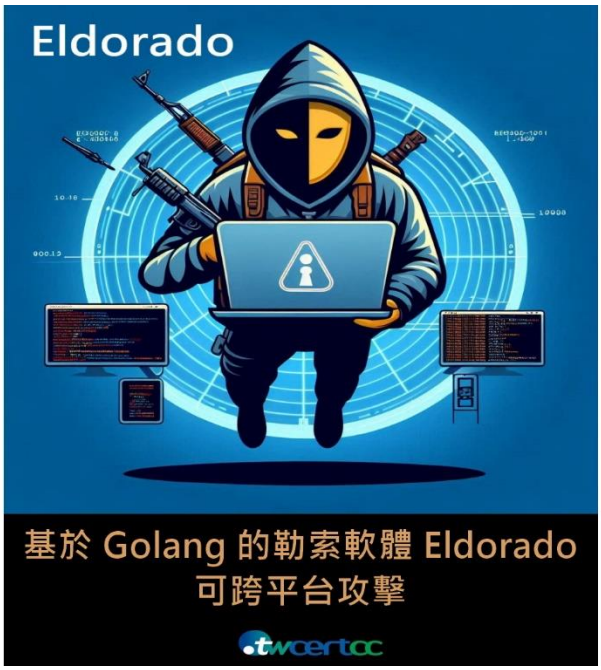
而從目前越來越多研究表明存在以PLC做為入侵端點，攻擊其他資訊系統，因此，在OT環境設置上，不能再無條件信任PLC發送的資料，同時也需要做好網路分段，避免所有人機介面(Human-Machine Interface,HMI)都可以跟 PLC 做連接，從而增加 PLC 被寫入惡意程式的可能性，也要盡量即時更新 OT 軟體，已避免存在已知漏洞能直接對 PLC 做寫入。

- 資料來源：

1. https://rt-solar.ru/solar-4rays/blog/4506/
2. https://rt-solar.ru/events/news/4509/
3. https://claroty.com/team82/research/white-papers/evil-plc-attack-weaponizing-plcs
4. https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Sole

2.2 資安趨勢

2.2.1 基於 Golang 的勒索軟體 Eldorado，可跨平台攻擊



資安業者 Group-IB Threat Intelligence 發現了一款基於Golang的勒索軟體-Eldorado，勒索軟體專門針對大型企業進行攻擊，並且具有跨平台攻擊能力，可攻擊 VMware ESXi、Windows 和 Linux 等多種系統。Eldorado 屬於勒索軟體即服務(Ransomware-as-a-Service,RaaS)，利用先進的方式加密金鑰及目標檔案，以SMB協定進行橫向擴散，並刪除特定檔案抹除加密痕跡及避免加密檔案被還原。

隨著科技的進步，攻擊者不斷探索新的攻擊方式，勒索軟體即服務已經演變成類似於大型企業的運作模式，這些勒索軟體組織持續在暗網論壇招募新的合作夥伴，並讓不同夥伴在團隊中執行特定任務。Eldorado 的相關訊息最初出現在俄羅斯的地下勒索軟體論壇 RAMP，當企業受駭後，Eldorado會透過暗網Onion 網域的聊天平台

與受駭者聯繫。截至 2024 年 6 月，全球已有 16 家公司遭到 Eldorado 攻擊，其中大部分位於美國，受影響的行業包括房地產、教育、專業服務、醫療保健和製造業等。

為了支援跨平台功能，Eldorado 使用 Golang 程式語言開發，讓其程式可在Windows與Linux的32bit及64bit系統中執行。此勒索軟體使用 Chacha20 演算法快速加密檔案，以Rivest Shamir Adleman-Optimal Asymmetric Encryption Padding(RSA-OAEP)加密金鑰，被加密的檔案其副檔名會被改為".00000001"，並在「文件」和「桌面」的目錄中建立名為「HOW_RETURN_YOUR_DATA.TXT」的文字檔案，裡面含有攻擊者的聯絡資訊。另Eldorado會透過 SMB 協定（SMB2/3）方式加密共用網路上的文件，且在加密完檔案後，使用 PowerShell 的命令，先以隨機位元的方式覆蓋加密器(encryptor)再刪除該檔案，以抹除相關加密的痕跡，最後也在系統中刪除windows的陰影複製(shadow copy)備份資料，防止受害電腦透過此機制復原被加密的檔案。

整體而言，儘管企業的網路安全意識不斷提高，但總有新形式的網路攻擊在不斷精進和發展。Group-IB 建議採取以下防禦措施：

- 採多重身份驗證（Multi-factor authentication,MFA）
- 建置端點偵測和回應（Endpoint Detection and Response,EDR），以協助識別勒索軟體的活動跡象
- 定期進行資料備份
- 使用人工智慧進行即時偵測入侵
- 定期更新系統並執行安全性修補
- 安排教育訓練，以幫助員工識別網路攻擊(如:釣魚郵件)
- 每年針對系統進行技術稽核或安全性評估

- 永遠不要支付贖金
- 受到攻擊時，尋求專家協助

Group-IB 強調，企業必須在網路安全工作中保持警覺和主動，以減輕這些不斷演變的威脅所帶來的風險。

- 資料來源：

1. Eldorado Ransomware: The New Golden Empire of Cybercrime?
2. New Eldorado ransomware targets Windows, VMware ESXi VMs
3. New Eldorado Ransomware Targets Multiple Sectors with Advanced Customization

2.3 軟硬體系統資安議題

2.3.1 GeoServer 漏洞曝光：開源地理位置資訊伺服器受到攻擊風險

近日全球廣泛使用的開源地理位置資訊伺服器GeoServer被發現存在嚴重的安全漏洞（CVE-2024-36401）。該漏洞源於GeoServer處理XPath表達式的方式，使得未經身份驗證的遠端攻擊者能夠利用這個漏洞在受影響的伺服器上執行任意代碼，從而獲取伺服器權限，近期已經發現有駭客利用漏洞進行攻擊，建議使用者儘速完成更新。

GeoServer是一個開源的地理空間資訊伺服器，允許用戶使用各種開放地理空間聯盟(Open Geospatial Consortium,OGC)標準發布和管理地理空間數據。GeoServer的功能強大且靈活，廣泛應用於政府、企業和學術機構。

CVE-2024-36401主要涉及GeoServer與GeoTools函式庫API之間參數傳送的內容，GeoServer在傳遞元素類型屬性名稱給commons-jxpath函式庫時存在不安全的操作，允許未經身份驗證的攻擊者注入特製的XPath表達式，導致可以執行任意程式碼。XPath是一種用於在XML文檔中選擇節點的語言，GeoServer使用的commons-jxpath函式庫，允許在Java中使用XPath表達式。這些技術的結合使GeoServer可以靈活地處理和查詢地理空間數據，但同時也引入了潛在的安全風險。GeoServer中XPath表達式評估的設計用途，原本應該只用於複雜特徵類型(如應用模式數據存儲)的 XPath 表達式評估，現在錯誤地被應用於簡單特徵類型，導致所有 GeoServer 實例都受到這個漏洞的影響。

在GeoServer中，WFS(Web Feature Service)是OGC定義的一個標準，用於在 Web 上共享地理空間資訊的標準化服務，它允許使用者通過 Web 服務查詢和擷取地理特徵的屬性資訊。在此漏洞中，WFS為攻擊者利用漏洞的一個入口點，攻擊者可以利用特製的請求觸發漏洞。 WFS功能中的WFS GetFeature、WFS GetPropertyValue、WMS GetMap、WMS GetFeatureInfo、WMS GetLegendGraphic 和 WPS Execute 均存在漏洞，未經身份驗證的遠端使用者可透過特製的輸入內容在預設的 GeoServer 中執行遠端程式碼(RCE)。

根據研究報告，GeoServer及GetTools影響的版本如下：

GeoServer

- •GeoServer< 2.23.6
- •2.24.0 <= GeoServer < 2.24.4
- •2.25.0 <= GeoServer < 2.25.2

GeoTools

- •GeoTools< 29.6
- •31.0 <= GeoTools < 31.2 程式碼執行

•30.0 <= GeoTools < 30.4

為了減輕CVE-2024-36401漏洞帶來的風險，可依下列方式修補GeoServer和GeoTools：

•刪除 gt-complex-x.y.jar 檔案：從 GeoServer 中刪除 gt-complex-x.y.jar 檔案，其中 x.y 為 GeoTools 版本(例如，如果運行 GeoServer 2.25.1，則刪除 gt-complex-31.1.jar)。此方法雖可提供臨時保護，但可能會影響 GeoServer 的某些功能。

•更新受影響的 JAR 檔案：修補版本已發布，用戶可以從 GeoServer 發布頁面下載受影響版本的 gt-app-schema、gt-complex 和 gt-xsd-core JAR 檔案。下載完畢後，只需用修補版本的檔案取代原始檔案即可。

- 資料來源：

1. https://nvd.nist.gov/vuln/detail/CVE-2024-36401
2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-36401
3. https://github.com/vulhub/vulhub/blob/master/geoserver/CVE-2024-36401/README.md
4. https://github.com/geoserver/geoserver/security/advisories/GHSA-6jj6-gm7p-fcvv
5. https://geoserver.org/announcements/vulnerability/2024/06/18/geoserver-2-25-2-released.html

2.3.2 大量Windows出現藍色當機畫面，資安公司CrowdStrike緊急修補更新程

2024年7月19日資安公司CrowdStrike的Falcon Sensor更新程式出現故障，導致全球各地Windows電腦出現藍色畫面當機(BSOD)狀況，全球企業和政府機關產生影響，包括航空公司、醫院、運輸機構及媒體公司等，許品Falcon Sensor市佔率為前幾名，因此這次更新問題導致大量Windows電腦多機構的運營受到嚴重干擾。CrowdStrike是知名的網路安全公司，其端點防護產陷入當機及系統重啟的循環，使得用戶無法正常使用電腦。

此次事件是由於Crowdstrike的Falcon平台派送有缺陷的更新所引起，導致已安裝該產品的某些版本Windows系統大範圍崩潰。許多企業反映其Windows電腦會自動重新啟動，並不斷循環地進入藍色當機畫面，其影響巨大，使全球的關鍵基礎設施營運產生嚴重衝擊，包含德國、日本、印度和美國的企業都出現類似問題。在台灣，許多公私立機關和企業也受到了影響，多家銀行、醫療機構及科技公司在事件發生後紛紛發現其系統無法正常運作，部分機構的業務運營因此中斷超過1小時。

CrowdStrike在發現問題後迅速做出了反應，發布了修補程式及解決方案。該公司表示這不是網路攻擊，問題的根源是某個Falcon Sensor更新檔案未經充分檢查所致。CrowdStrike已經刪除錯誤更新檔案並發布了修補程式，用戶可透過官方網站提供的步驟回復系統(可參考相關連結)。

此外，微軟針對此當機狀況提出2個復修方式，分別是「從WinPE復原」及「從安全模式復原」。若選擇從「從WinPE復原」，可以快速並直接復原系統，不需要系統管理者的權限，但系統已透過BitLocker或第三方軟體加密時，需先解除加密狀況才能修復受影響的系統。若選擇「從安全模式復原」，則需使用本地管理者權限的使用者登入後進行修復。需要注意的是，在復修之前需先下載已簽署的Microsoft Recovery Tool，並透過工具中的powershell檔案建立USB開機碟。

全球資訊科技研究顧問公司 Gartner 指出，企業即使在此次事件未受影響，以安全性的角度來看，仍需關注其帶來的影響，以防範未來類似事件的發生。Gartner 同時建議企業應重視資安事件的應變措施，資安事件發生時的相關處理措施如下：

- 立即採取行動（第一到七天）：

【事件應變與危機管理】

1. 通知危機管理團隊，讓其參與並協助應處
2. 通過有效的危機溝通通知所有利害關係人
3. 驗證資訊來源以避免遭受二次網路攻擊
4. 動員危機管理團隊以防止使用者操作失誤
5. 指派專門的溝通團隊進行內部利害關係人的協調
6. 讓安全運營團隊參與監控和應對新威脅

【技術修復】

1. 讓 IT 專業人員幫助使用者解決問題
2. 建立分類流程，以對資產進行分類並確定設備修復的優先順序
3. 利用資產管理工具識別並列出已離線的設備
4. 避免過度反應，例如完全停用或替換CrowdStrike

- 中期行動（第1到2週）：

【評估影響與安全】

1. 與 SOC 團隊一起檢視異常情況，以降低未檢測到的攻擊風險
2. 參與營運衝擊分析會議，一同討論潛在的安全風險
3. 向公司中高階領導報告設備的狀況，並持續提供穩定的環境
4. 盡量讓端點保護工具在佈署更新檔時能先行測試，減少更新失敗的狀況
5. 可透過輪班或其它方式，以減輕員工的壓力及倦怠感

- 長期行動（第8 至 12 週）

【韌性和準備】

1. 重新審視公司在發生大規模主機當機時的預防、回應和支援程序
2. 檢查並更新停機程序，並根據需要修訂危機溝通計劃、事件反應流程及災害復原和持續營運計畫
3. 確保關鍵員工有能力並參與測試企業系統

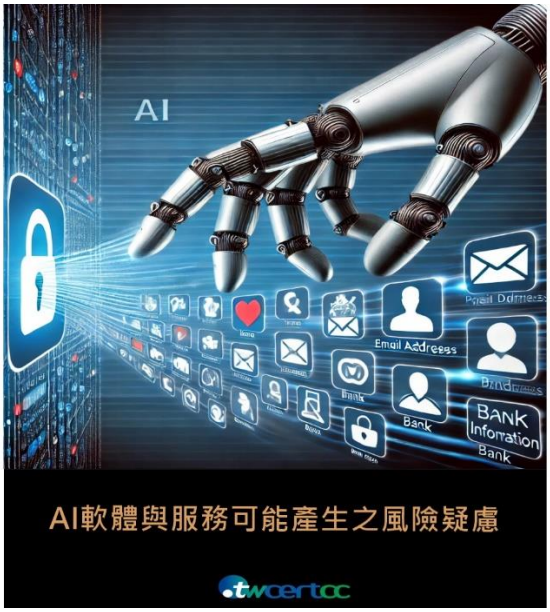
4. CrowdStrike 的停機事件強調了專注於韌性的必要性，必需建立全面性的策略目標
5. 部署安全產品前評估其效益，選擇合適的工具以改善現有的防護機制

- 資料來源：

1. https://www.crowdstrike.com/blog/falcon-update-for-windows-hosts-technical-details/
2. https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/
3. https://techcommunity.microsoft.com/t5/intune-customer-success/new-recovery-tool-to-help-with-crowds
4. https://www.cityam.com/a-blue-screen-of-death-loop-how-a-crowdstrike-update-crashed-microsoft-system
5. https://www.linkedin.com/pulse/ode-outage-jen-easterly-2dcse?utm_source=share&utm_medium=member_ios&utm_campaign=share_via
6. https://www.youtube.com/watch?v=Bn5eRUaMZXk&ab_channel=CrowdStrike

2.4 資訊安全宣導

2.4.1 AI軟體與服務可能產生之風險疑慮



近年來AI軟體與服務快速發展，影響遍及全球產官學研各界。自ChatGPT於2022年底發布後，更掀起全球熱潮，且被視為人工智慧之一項重大突破。運用生成式AI軟體與服務協助執行業務或提供服務，有助於提升工作效率與創意發想。

AI軟體與服務常透過蒐集使用者輸入內容或擷取網頁文字做為訓練資料，以逐步改善模型並產出更正確之結果，故可能涉及隱私洩露之風險。另外，AI軟體與服務透過大量蒐集與訓練所產出之結果，可能涉及侵害智慧財產權、人權或商業機密之風險，且受限於訓練資料之品質與數量，可能會生成真偽難辨或創造不存在之資訊，建議針對生成結果需進行評估後再行運用。

使用AI軟體與服務時，應避免暴露個人資料與機敏資訊，同時注意內部保密義務與智慧財產權相關規定，秉持負責任及可信賴之態度，掌握自主權與控制權，並堅守安全性、隱私性與資料治理、問責等原則，不得恣意揭露未經公開之公務資訊、不得分享個人隱

私資訊及不可完全信任生成資訊。

此外，有鑑於過往曾發生軟體與APP被發現重大資安疑慮情事，近期AI軟體與服務如雨後春筍般誕生之際，亦難免出現相似資安疑慮，因此選用AI軟體與服務時，需留意提供該軟體與服務之公司背景，不應盲目信任使用。

隨著針對不同使用情境不斷推陳出新之AI軟體與服務，建議企業與民眾使用前審慎評估軟體是否安全，輸入之資料是否敏感，並了解軟體開發商之隱私權政策及如何處理資安漏洞等問題，以免發生違法、洩漏敏感資訊、侵害智慧財產權及財物損失之憾事。若欲於工作中採用AI軟體與服務，可參考「行政院及所屬機關（構）使用生成式AI參考指引(草案)」，以降低可能帶來之危害與風險。

- 資料來源：
  1. 行政院及所屬機關(構)使用生成式 AI 參考指引

2.5 軟硬體漏洞資訊

2.5.1 Linux kernel存在高風險安全漏洞

CVE 編號	CVE-2022-2586
影響產品	Linux 平台
解決辦法	官方已針對漏洞釋出修補程式，網址如下： https://lore.kernel.org/netfilter-devel/20220809170148.164591-1-cascardo@canonical.com/T/ 因使用 Linux 的作業系統眾多，更新方式請參考對應廠商公告，以下列舉常見作業系統之官方說明： Ubuntu｜https://ubuntu.com/security/CVE-2022-2586 Debian｜https://security-tracker.debian.org/tracker/CVE-2022-2586 Red Hat｜https://access.redhat.com/errata/RHSA-2024:0724 Fefora｜https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/DUQKTPH7LFK5E2J3I73LHDSUS2357P3U/

- 內容說明：

  研究人員發現 Linux kernel 之 nft 資料表(NF_Tables)存在記憶體釋放後使用漏洞(Use After Free)漏洞(CVE-2022-2586)，已取得一般權限之本機端攻擊者可利用此漏洞提升至管理員權限。該漏洞已遭駭客利用，請儘速確認並進行修補。

- 影響平台：

  Linux kernel 5.19.17(含)以前版本

- 資料來源：

1. https://nvd.nist.gov/vuln/detail/CVE-2022-2586
2. https://ubuntu.com/security/CVE-2022-2586
3. https://security-tracker.debian.org/tracker/CVE-2022-2586
4. https://access.redhat.com/errata/RHSA-2024:0724
5. https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/DUQKTPH7LFK5E2J3I73LHDSUS2357P3U/

2.5.2 OpenSSH存在高風險安全漏洞

CVE 編號	CVE-2024-6387
影響產品	OpenSSH
解決辦法	請升級 OpenSSH 至 9.8p1(含)以上版本。

- 內容說明：

  研究人員發現 OpenSSH 存在競爭條件(Race Condition)漏洞(CVE-2024-6387)，允許未經身分鑑別之遠端攻擊者可利用此漏洞執行任意程式碼，該漏洞已遭駭客利用，請儘速確認並進行修補。

- 影響平台：

  OpenSSH 8.5p1 至 9.7p1 版本

- 資料來源：

  1. https://nvd.nist.gov/vuln/detail/CVE-2024-6387
  2. https://www.openssh.com/txt/release-9.8
  3. https://www.ithome.com.tw/news/163737

2.5.3 GeoServer存在高風險安全漏洞

CVE 編號	CVE-2024-36401
影響產品	GeoServer
解決辦法	官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下： https://github.com/advisories/GHSA-6jj6-gm7p-fcvv

- 內容說明：

  研究人員發現 GeoServer 存在程式碼注入(Code Injection)漏洞(CVE-2024-36401)，未經身分鑑別之遠端攻擊者可利用此漏洞遠端執行任意程式碼。該漏洞之概念驗證(PoC)已被公開，請儘速確認並進行修補。

- 影響平台：
  - Geoserver 2.23.6(不含)以前版本
  - Geoserver 2.24.0 至 2.24.4(不含)版本
  - Geoserver 2.25.0 至 2.25.2(不含)版本

- 資料來源：
  1. https://github.com/advisories/GHSA-6jj6-gm7p-fcvv

2.5.4 GeoServer之開源專案JAI-EXT存在高風險安全漏洞

CVE 編號	CVE-2022-24816
影響產品	GeoServer
解決辦法	官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下： https://github.com/geosolutions-it/jai-ext/security/advisories/GHSA-v92f-jx6p-73rx

- 內容說明：

  研究人員發現在 GeoServer 之開源專案 JAI-EXT 中，其 jt-jiffle 套件存在程式碼注入(Code Injection)漏洞(CVE-2022-24816)，未經身分鑑別之遠端攻擊者可利用此漏洞遠端執行任意程式碼。該漏洞已遭駭客利用，請儘速確認並進行修補。

- 影響平台：

  jt-jiffle 套件 1.1.22(不含)以前版本

- 資料來源：

  1. https://nvd.nist.gov/vuln/detail/CVE-2022-24816
  2. https://github.com/geosolutions-it/jai-ext/security/advisories/GHSA-v92f-jx6p-73rx
  3. https://github.com/geosolutions-it/jai-ext/commit/cb1d6565d38954676b0a366da4f965fef38da1cb

2.5.5 Microsoft Windows MSHTML Platform存在高風險安全漏洞

CVE 編號	CVE-2024-38112
影響產品	Windows
解決辦法	官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下： https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112

- 內容說明：

  研究人員發現 Microsoft Windows MSHTML Platform 存在遠端執行程式碼(Remote Code Execution)漏洞(CVE-2024-38112)，允許未經身分鑑別之遠端攻擊者誘騙使用者下載惡意檔案後，利用此漏洞執行任意程式碼。該漏洞已遭駭客利用，請儘速確認並進行修補。

- 影響平台：
  - Windows 10 for 32-bit Systems
  - Windows 10 for x64-based Systems
  - Windows 10 Version 1607 for 32-bit Systems
  - Windows 10 Version 1607 for x64-based Systems
  - Windows 10 Version 1809 for 32-bit Systems
  - Windows 10 Version 1809 for ARM64-based Systems
  - Windows 10 Version 1809 for x64-based Systems
  - Windows 10 Version 21H2 for 32-bit Systems
  - Windows 10 Version 21H2 for ARM64-based Systems
  - Windows 10 Version 21H2 for x64-based Systems
  - Windows 10 Version 22H2 for 32-bit Systems
  - Windows 10 Version 22H2 for ARM64-based Systems
  - Windows 10 Version 22H2 for x64-based Systems
  - Windows 11 version 21H2 for ARM64-based Systems
  - Windows 11 version 21H2 for x64-based Systems
  - Windows 11 Version 22H2 for ARM64-based Systems
  - Windows 11 Version 22H2 for x64-based Systems

- Windows 11 Version 23H2 for ARM64-based Systems
- Windows 11 Version 23H2 for x64-based Systems
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Server 2016 (Server Core installation)
- Windows Server 2019
- Windows Server 2019 (Server Core installation)
- Windows Server 2022
- Windows Server 2022 (Server Core installation)
- Windows Server 2022, 23H2 Edition (Server Core installation)

- 資料來源：
  1. https://nvd.nist.gov/vuln/detail/CVE-2024-38112
  2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112
  3. https://www.trendmicro.com/en_us/research/24/g/CVE-2024-38112-void-banshee.html

2.5.6 Cisco 思科郵件安全閘道(Secure Email Gateway)存在高風險安全漏洞

CVE 編號	CVE-2024-20401
影響產品	Cisco Secure Email Gateway
解決辦法	思科已發布更新軟體予以修補，並強調沒有其他替代的緩解措施。請更新 Content Scanner Tools 至 23.3.0.4823 (含)之後版本。

- 內容說明：

  Cisco Secure Email Gateway 存在任意檔案寫入漏洞，該漏洞是因開啟文件分析及內容過濾功能時，不當處理郵件附檔造成。該漏洞可能允許未經驗證的遠端攻擊者，藉由寄送帶有特製附件的惡意郵件觸發漏洞，從而新增具有 root 權限的使用者、竄改裝置組態、執行任意程式碼，或在受影響的裝置上造成永久阻斷服務 (DoS) 。

- 影響平台：

  在寄入信件(incoming mail)設定中，開啟文件分析及內容過濾功能時，若 Content Scanner Tools 版本低於 23.3.0.4823(不含)

- 資料來源：

  1. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-bGG2U

2.5.7 Cisco 思科SSM On-Prem存在高風險安全漏洞

CVE 編號	CVE-2024-20419
影響產品	Cisco Smart Software Manager On-Prem
解決辦法	思科已發布更新軟體予以修補，並強調沒有其他替代的緩解措施。請更新 Cisco Smart Software Manager On-Prem 至 Versions 8-202212 (含)之後版本。

- 內容說明：

  Smart Software Manager On-Prem 存在 Password Change 漏洞，該漏洞可能允許未經驗證的遠端攻擊者變更任何使用者的密碼，包括具有管理權限的使用者。

  該弱點是因密碼更改程序處理不當造成，攻擊者可以藉由向受影響的設備發送特製的 HTTP 請求利用該弱點，成功利用該漏洞可能會允許攻擊者以受害使用者的權限存取 Web UI 或 API。

- 影響平台：

  Cisco Smart Software Manager On-Prem 8-202206 (含)之前版本

- 資料來源：

  1. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-auth-sLw

第 3 章、資安研討會及活動

【限定資訊服務業者參與】2024-03-26 ~ 2024-09-30 個人資料檔案安全維護計畫一對一線上健檢諮詢	
活動時間	2024-03-26 ~ 2024-09-30
活動地點	線上活動
活動網站	https://www.cisanet.org.tw/Course/Detail/5286
活動概要	 【活動內容 / Event Deails】 數產署於 2024 年 10 月 12 日訂定「數位經濟相關產業個人資料檔案安全維護管理辦法」，業者若未採取適當安全維護措施致個資被竊取、竄改、毀損、滅失或洩漏，或未訂定安全維護計畫，可處 2 萬元以上 200 萬元以下罰鍰！ 為協助資訊服務業者遵循《數位經濟相關產業個人資料檔案安全維護管理辦法》，建立個資檔案安全維護管理計畫，數產署提供線上免費個資健檢諮詢，名額有限，敬請把握。 【指導單位】 數位發展部數位產業署 【主辦單位】財團法人資訊工業策進會 【執行單位】中華民國資訊軟體協會 【聯絡窗口】02-2553-3988 分機 816 林專員 security@cisanet.org.tw

【資安學院】8/6 Linux鑑識處理(實作課)	
活動時間	**2024-08-06 09:00 ~ 17:00**
活動地點	**中華民國資訊軟體協會-大同辦公室D01大會議室（台北市中山區中山北路3段22-1號新設工大樓 5樓 C區）**
活動網站	**https://www.cisanet.org.tw/Course/Detail/5265**
活動概要	 **【費用】** 原價：NT 8,400元/人 早鳥價：NT 7,600元/人(開課前一個月需完成報名) 軟協會員價：NT 6,800元/人 費用含稅、教材、餐點及完課證明 **【活動內容 / Event Deails】** 於Linux系統開源之特性， Linux作業系統主機廣泛地為政府企業所採納，用於架設網站伺服器及郵件伺服器以提供服務，與此同時，Linux主機系統逐漸成為駭客覬覦的目標，針對Linux系統主機的駭客攻擊層出不窮。 本課程旨在透過模擬Linux系統受駭的情境，使學員瞭解駭客針對Linux系統可能發動的攻擊，及相關工具進行鑑識處理，以精進Linux作業系統之鑑識處理能力，並掌握Linux作業系統最新資安威脅態樣。

	【主辦單位】中華民國資訊軟體協會 【聯絡窗口】02-2553-3988 分機 816 林專員 security@cisanet.org.tw 【報名截止】2024-07-30

【資安學院-國際證照班】8/15-8/16、8/21-8/23 ISO/IEC 27001:2022 資訊安全管理系統 CQI & IRCA 主導稽核員訓練課程	
活動時間	**2024/8/15-8/16、8/21-8/23 09:00-18:30**
活動地點	**中華民國資訊軟體協會-大同辦公室D01大會議室（台北市中山區中山北路3段22-1號新設工大樓 5樓 C區）**
活動網站	**https://www.cisanet.org.tw/Course/Detail/5177**
活動概要	 **【費用】** 原價：NT 56,000元/人 早鳥價：NT 53,000元/人(開課前一個月需完成報名) 公務機關/關鍵基礎設施/軟協會員：請致電承辦人 費用含稅、教材、餐點及完課證明 **【活動內容 / Event Deails】** 備受國際認可的 ISO/IEC 27001 是一套出色的資訊安全管理框架，可幫助組織有效管理和保護資訊資產。取得此證照不僅代表個人在資安管理上，建置與稽核專業之肯定，更代表企業組織內部中，其資安專業種子人才能力的展現！ **【主辦單位】**中華民國資訊軟體協會 **【聯絡窗口】**02-2553-3988 分機 816 林專員　security@cisanet.org.tw **【報名截止】**2024-08-08

【資安學院-國際證照班】9/2 BS 10012:2017+A1:2018 個人資訊管理系統基礎課程	
活動時間	**2024-09-02 09:00 ~ 2024-09-02 17:00**
活動地點	**中華民國資訊軟體協會-大同辦公室D01大會議室（台北市中山區中山北路3段22-1號新設工大樓 5樓 C區）**
活動網站	**https://www.cisanet.org.tw/Course/Detail/5303**
活動概要	 **【費用】** 原價：8,500元/人 早鳥價： NT 8,450元/人(開課前兩個月需完成報名及繳費) 軟協會員：請洽承辦人員 費用含稅、教材、餐點及完課證明 **【活動內容 / Event Deails】** 本課程為學習個人資訊管理系統 (PIMS) 的最佳入門課程。學員可經由課程了解個人資訊的重要性，讓各個規模的組織在短時間內瞭解個資管理系統，及國內法令法規要求，對資料保護原則及範圍有初步且正確的認知。並且能協助組織達到加深完善個資管理作業流程及正確因應新版個資法之益處。 **【主辦單位】**中華民國資訊軟體協會 **【聯絡窗口】**02-2553-3988 分機 816 林專員　security@cisanet.org.tw **【報名截止】**2024-08-26

【資安學院-國際證照班】9/19-9/20 ISO/IEC 27001:2022資訊安全管理系統 主導稽核員「轉版」訓練課程（二日）	
活動時間	2024-09-19 09:00 ~ 2024-09-20 17:00
活動地點	中華民國資訊軟體協會-大同辦公室D01大會議室（台北市中山區中山北路3段22-1號新設工大樓 5樓 C區）
活動網站	https://www.cisanet.org.tw/Course/Detail/5179
活動概要	 **【費用】** 原價：NT 24,000元/人 早鳥價： NT 23,500元/人(開課前兩個月需完成報名) 公務機關/軟協會員：請致電承辦人

	費用含稅、教材、餐點及完課證明 **【活動內容 / Event Deails】** ISO 27001 隨著數位化改變全球數位格局，如遠端工作、自攜電子設備以及工業 5.0 等商業實務，變得更佳依賴雲端和數位。ISO/IEC 27001 於 2022 年 10 月 25 日正式頒佈新版標準（2022 年版），本次轉課程將協助您快速掌握附錄 A 條款五至八的變化，並能夠幫助組織因應新版 ISO/IEC 27001:2022 標準，以此展現組織資安風險控管績效並強化客戶信任。 **【主辦單位】**中華民國資訊軟體協會 **【聯絡窗口】**02-2553-3988 分機 816 林專員　security@cisanet.org.tw **【報名截止】**2024-09-12

第 4 章、TVN 漏洞公告

TWCERT/CC 本月份發布之CVSS 3分數為8.8以上之漏洞資訊如下表：

二一零零科技 電子公文檔案管理系統 - Broken Access Control	
TVN / CVE ID	TVN-202407003 / CVE-2024-6737
CVSS	8.8 (High) CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
影響產品	電子公文檔案管理系統 5.0.77(不含)以前版本
問題描述	二一零零科技電子公文檔案管理系統的存取控制並未實作完善，可讓已取得一般權限之遠端攻擊者存取帳號設定功能並新增管理員帳號。
解決方法	更新至 5.0.77 (含)以後版本 (112/4/20 釋出)
公開日期	2024-07-15
相關連結	**https://www.twcert.org.tw/tw/cp-132-7923-46df3-1.html**

全識科技 空間管理系統 - SQL injection	
TVN / CVE ID	TVN-202407009 / CVE-2024-6743
CVSS	9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
影響產品	空間管理系統 2024-04-09-3302(不含)以前版本
問題描述	全識科技的空間管理系統未妥善驗證使用者輸入，允許未經身分鑑別之遠端攻擊者注入任意 SQL 指令讀取、修改及刪除資料庫內容。
解決方法	更新至2024-04-09-3302(含)以後版本

公開日期	2024-07-15
相關連結	https://www.twcert.org.tw/tw/cp-132-7932-a6d4d-1.html

基點資訊 Secure Email Gateway - Stack-based Buffer Overflow	
TVN / CVE ID	TVN-202407010 / CVE-2024-6744
CVSS	9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
影響產品	Secure Email Gateway 4.5.0(含)以前版本
問題描述	基點資訊 Secure Email Gateway 其 SMTP Listener 未能有效驗證使用者輸入導致Buffer Overflow漏洞，未經身分鑑別之遠端攻擊者可利用此漏洞於遠端伺服器上執行任意系統指令。
解決方法	安裝修補程式 Build_20240529(含)以後版本
公開日期	2024-07-15
相關連結	https://www.twcert.org.tw/tw/cp-132-7936-f6381-1.html

中華數位科技 Mail SQR Expert 與 Mail Archiving Expert - OS Command Injection	
TVN / CVE ID	TVN-202407011 / CVE-2024-5670
CVSS	9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
影響產品	SN OS 12.1 230921(含)以前版本 SN OS 12.3 230921(含)以前版本 SN OS 10.3 230630(含)以前版本
問題描述	中華數位科技 Mail SQR Expert 與 Mail Archiving Expert之網頁服務未妥善驗證使用者輸入，允許未經身分鑑別之遠端攻擊者注入任意OS指令並於遠端伺服器上執行。

解決方法	更新 SN OS 12.1 至 230922(含)以後版本 更新 SN OS 12.3 至 230922(含)以後版本 更新 SN OS 10.3 至 230631(含)以後版本 受影響產品若執行於FreeBSD 9.x將不支援更新，請先更新作業系統版本。
公開日期	2024-07-29
相關連結	**https://www.twcert.org.tw/tw/cp-132-7958-817f4-1.html**

達煬科技 WinMatrix3 Web 套件 - SQL Injection	
TVN / CVE ID	TVN-202407012 / CVE-2024-7201
CVSS	9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
影響產品	WinMatrix3 Web套件1.2.33.3(含)以前版本
問題描述	達煬科技 WinMatrix3 Web 套件之登入功能未妥善驗證使用者輸入，允許未經身分鑑別之遠端攻擊者注入SQL指令讀取、修改及刪除資料庫內容。
解決方法	請更新至WinMatrix3 Web套件1.2.35.3(含)以後版本
公開日期	2024-07-29
相關連結	**https://www.twcert.org.tw/tw/cp-132-7960-0ee18-1.html**

達煬科技 WinMatrix3 Web 套件 - SQL Injection	
TVN / CVE ID	TVN-202407013 / CVE-2024-7202
CVSS	9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
影響產品	WinMatrix3 Web套件1.2.33.3(含)以前版本

問題描述	達煬科技 WinMatrix3 Web 套件之查詢功能未妥善驗證使用者輸入，允許未經身分鑑別之遠端攻擊者注入SQL指令讀取、修改及刪除資料庫內容。
解決方法	請更新至WinMatrix3 Web套件1.2.35.3(含)以後版本
公開日期	2024-07-29
相關連結	**https://www.twcert.org.tw/tw/cp-132-7962-dd216-1.html**

編輯：**TWCERT/CC 團隊**

發行單位：**台灣電腦網路危機處理暨協調中心**

(Taiwan Computer Emergency Response Team / Coordination Center)

出刊日期：**2024年 7月 30 日**

電子郵件：**CERT_Service@cert.org.tw**

官網：**https://twcert.org.tw/**

Facebook 粉絲專頁：**https://www.facebook.com/twcertcc/**

Instagram：**https://www.instagram.com/twcertcc/**