TWCERT/CC 資安情資電子報

2024 年 5 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。範疇包含資安趨勢、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

第 1 章、封面故事

駭客針對Openfind產品發動攻擊

國家資通安全研究院分析近期攻擊攻擊活動，發現駭客針對網擎資訊Mail2000電子郵件系統與MailGates郵件防護系統進行攻擊，透過產品漏洞入侵企業織組織，Openfind網擎資訊針對通報漏洞皆已提供修補程式，請留意Openfind更新資訊。

本月初再度發現駭客對Openfind Mail2000產品進行了零日攻擊，該漏洞主要是由於login_lock_notification.dat未對Login進行緩衝區溢位進行處理，駭客可以繞過檢查並執行JavaScript，從而導致XSS(Reflected Cross-site scripting)安全漏洞，網擎公司偵測發現後，已完成修補並釋出更新，以維護客戶的權益。

同期間亦發現駭客利用CVE-2022-30333漏洞對網擎公司MailGates郵件防護系統進行攻擊，網擎公司為強化MailGates產品安

全性，持續釋出安全性更新，並宣導用戶更新至最新版本。

Openfind網擎資訊是一家專注於開發搜尋引擎技術和相關網路應用服務的公司。目前他們為許多重要政府機關和大型企業客戶提供服務。近期發現駭客對Mail2000電子郵件系統和MailGates郵件防護系統發動零時差漏洞攻擊。Openfind公司的電子郵件威脅實驗室已經立即針對這一情況展開研發工作，以更新的方式協助所有客戶立即降低相關風險。

資訊系統漏洞為駭客利用入侵重要管道之一，因此定期更新漏洞為企業組織資訊人員非常重要工作項目，可確保系統安全的重要措施，有助於防止資料外洩、系統毀損，以及駭客攻擊，同時維護組織的聲譽。

- 資料來源：
  1. 網擎資訊-程式更新

第 2 章、國內外重要資安事件

2.1 資訊安全宣導

2.1.1 建立安全的雲端環境：身分認證與存取管理實務(下)

面對雲端安全的挑戰，除了透過身份認證方式管控外，CISA同時提出身分識別與存取管理(Identity and Access Management, IAM)策略，安全性應放在使用雲端技術時的首要位置，透過嚴格的身份和存取管理實務，有效地保護雲端環境免受潛在的攻擊威脅, 本篇文章將繼續介紹CISA所提出的存取控制策略重點，來確保雲端資料的安全與完整性。

存取管理(Access management)

- **管理條件性存取(Managing conditional context-based access)**

儘管透過安全的密碼、實體驗證設備和多因子認證(Multi-Factor Authentication, MFA)對保護使用者帳戶很重要，但惡意網路攻擊者

(Malicious cyber actors, MCAs)仍可能對使用者的帳戶安全構成威脅。為了應對這些威脅，其中一種方法是根據額外的資訊來限制存取，這些資訊通常在政策中定義，可以根據特定條件來限制使用者登入系統的權限，例如，根據來源 IP 位址來阻止未授權地區的嘗試登入。

這些控制措施對於保護特權帳戶（或者擁有廣泛/敏感存取權限的帳戶）至關重要，因為它強制要求管理員只能從組織的本地設施登入這些帳戶。組織應該對其設定的存取限制進行全面稽核和測試，以防止攻擊者利用政策中的漏洞。

- **存取資源的加密通道(Encrypted channels for accessing resources)**

在儲存雲端資料時，存取控制是非常重要的。未經授權的存取可能會降低整體安全性，並對運營產生負面影響。為了確保存取資料的安全性，我們可以採取以下措施：

- 確保權限分配符合最小權限原則，並持續驗證存取和管理權限
- 啟用對存取請求和策略變更的監控和記錄
- 及時調查異常活動，以確保資料的安全性
- 使用加密技術保護靜態和傳輸中的資料，並妥善儲存和管理加密金鑰
- 使用 TLS1.2 或更高版本的安全協議，盡可能使用商業國家安全演算法 (CNSA) Suite 2.0 中的演算法，並至少使用 CNSA Suite 1.0 來進行客戶端與雲端資源的連接

- **職責分離(Separation of duties)**

分離職責是保護雲端資源的關鍵概念， NIST 將職責分離定義為「不應該授予使用者足夠的權限來單獨濫用系統」。落實這個原則的其中一種方式，是在執行特別敏感操作時需要兩個人控制。另一種方法是透過分離管理員角色來控制資源的存取和管理。例如，金

鑰管理服務（Key Management System, KMS）的存取控制管理員擁有授予對保護敏感資料或功能的金鑰所需的權限。然而，這些管理員不應該允許自己被授予可以存取金鑰。儘管某些情況下，一般使用者可能需要建立、管理和使用自己的加密金鑰，但這是提高組織敏感資料安全性的重要方法。

此外，應限制備份資料的寫入權限，以對抗惡意攻擊者用於備份資料的勒索軟體戰術、技術、程序（TTP）。降低雲端環境資料備份外洩風險的其中一種方法，是為需要存取備份檔案的管理員，建立獨立的備份管理帳戶。這些預防措施限制了具有存取憑證的內部威脅者或惡意攻擊者，對受感染的雲端環境造成更多影響。

- **使用者資料保護(User data protections)**

控制使用者設備是惡意攻擊者取得組織雲端環境存取權限的常見攻擊途徑，對於雲端使用者來說，在使用裝置存取雲端資源時，應注意保持良好的網路安全習慣，並採取以下措施：

- 定期更新作業系統與應用程式
- 避免打開來自未知寄件者的電子郵件與連結，以減少網路釣魚和惡意軟體感染的風險
- 變更和刪除預設設定（例如預設密碼與預設使用者帳戶）
- 監控帳戶是否有異常的活動
- 檢查URL是否有被修改過，其目的在將使用者引導到偽造的網站
- 考慮使用者使用未受管理的設備（如自攜設備或個人電腦）存取雲端資源的風險和利益

- **權限控制(Privilege controls)**

大多數的雲端服務提供商(Cloud Service Provider, CSP)使用兩種

方法的混合形式來強化控制存取，一是基於角色的存取控制(Role-based access controls, RBAC)，另一種是基於屬性的存取控制(ABAC)。在使用基於角色的存取控制(RBAC)時，組織會給予角色權限，然後將使用者指派給這些角色，從而授予使用者相應的權限。如果角色的權限發生變更，所有分配了該角色的人都會受到影響。而基於屬性的存取控制(ABAC)則是根據使用者和資源的屬性來控制對資料的存取，提供了比單獨使用RBAC策略更細緻的資源策略保護。

對權限進行規則化是管理企業權限和偵測偏差的其中一種方法，稱為政策即程式碼(Policy as Code, PaC)。這對企業權限管理非常有用，因為它可依現存良好狀態建立相關權限的設定，未來可進行審核和版本控制，並可用於偵測偏差(drift)。有關在雲端環境中使用政策即程式碼的更多詳細信息，可參閱NSA CSI：透過基礎設施即程式碼實施安全自動化部署實務。除了政策即程式碼之外，身份管理系統也能根據業務需求自動分配角色。

考慮實施即時(Just-in-Time, JIT)安全實務，欲提昇應用程式或系統的存取權限，應僅限於預先指定的時段及行為。JIT提升特權時，應該被記錄下來，且需有正當理由，若能追蹤及驗證所要求的權限更好。

最後，避免使用特權帳戶進行日常活動，僅使用特權帳戶進行維護、更新、帳戶管理、威脅狩獵等需要特權存取的作業。定期審核身分識別與存取管理的設定，以確認使用者僅被授予必要的權限。許多雲端服務提供商提供的服務會追蹤未使用的權限，以幫助管理員根據使用者完成日常職責所需，給予最低的權限。但是，在刪除看似未使用的權限時，也需考慮到偶爾或緊急存取的狀況。

- **保護個體中繼資料服務(Securing the cloud instance metadata service)**

個體中繼資料服務(Instance Metadata Service, IMDS)允許虛擬實

例查詢租戶相關資訊，然而，這個服務可能被惡意使用，以獲取雲端租戶身分識別與存取管理(IAM)憑證的額外存取權限。通常情況下，惡意攻擊者會利用客戶組織在雲端實例中運行應用程式的伺服器端請求偽造(SSRF)漏洞來查詢IMDS。為了防止這種情況發生，應該採用已知的最佳實務來保護應用程式，例如過濾用戶輸入的資料、配置 Web 應用程式防火牆，僅開放需要的實例或帳戶存取IMDS。每個雲端服務提供商的IMDS可能稍有不同，因此，重要的是查閱供應商關於他們的IMDS的最佳實踐指南，以採取所有可能的預防措施來防止服務被誤用。

最佳實務(Best practices)

在雲端運作的組織應該讓員工了解，不當的身分識別和存取管理所造成的安全性問題，以降低資安風險。以下是一些最佳實務建議：

- **身分識別管理**

- 強制使用多因子認證(MFA)，提高使用者帳戶的安全性。
- 不要將伺服器 TLS 憑證以明文形式儲存在托管 Web 伺服器的虛擬實例上；應使用密鑰管理器來保護它們。
- 謹慎處理使用者的 PKI 憑證，避免未經授權的取得相關憑證，並及時撤銷被不當取得或不必要的憑證。
- 限制金鑰的使用，僅在需要時提供短期存取權限，並以配置最少的必要權限。
- 保護身分聯合伺服器並定期審核身分聯合，以偵測惡意使用者企圖濫用信任關係。

- **存取管理**

- 使用基於上下文的存取控制策略，並定期稽核以識別潛在的漏

洞。

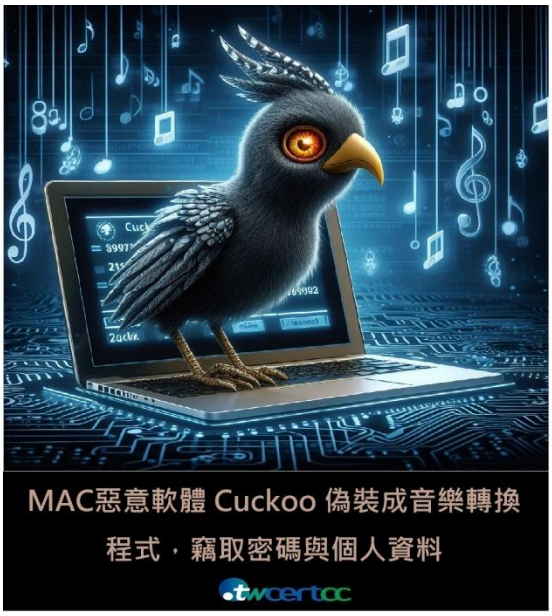
- 考慮是否要求管理員使用特權訪問工作站(Privileged Access Workstation, PAW)來存取雲端資源。
- 限制管理帳戶的使用，並使用 JIT (Just-In-Time) 存取來限制特權存取，以改善對特權操作的追蹤。
- 使用安全協議(如 TLS 1.2 或更高版本)和經過批准的密碼套件(最好是CNSA Suite 2.0)來加密通道，並用以連接到雲端資源。
- 根據存取控制的最佳實踐分配權限，遵行職責分離和最小權限原則，並定期審核權限分配和存取請求。
- 考慮使用政策即程式碼來改進存取控制策略的追蹤和稽核，並經常檢查偏差(drift)。
- 透過限制使用者/服務對 IMDS 的查詢權限、使用最新版本、實施供應商特定的最佳實務以及實施適當的安全措施來保護雲端託管應用程式並防止 SSRF 漏洞，從而保護雲端 IMDS。

雲端安全的身份認證和存取控制是確保在雲端環境中資料安全的重要方式之一，而定期的監控、日誌記錄和安全事件應變也是確保雲端安全的重要措施，企業在享受雲端技術的方便性時，亦能透過嚴謹的管理機制保護企業資料安全。

- 資料來源：
  1. Use Secure Cloud Identity and Access Management Practices

2.2 新興應用資安

2.2.1 MAC惡意軟體 Cuckoo 偽裝成音樂轉換程式，竊取密碼與個人資料



Cuckoo惡意程式透過偽裝成音樂轉載程式，引誘使用者下載檔案，攻擊 macOS的用戶，以竊取使用者密碼、歷史瀏覽紀錄、加密貨幣錢包詳細訊息等。

資安研究人員 Kandji 最近發現專門針對 Apple macOS 系統的新型資訊竊取程式「Cuckoo」，這款惡意程式偽裝成音樂轉換應用程式，聲稱可擷取串流媒體上的音樂，並轉換為mp3格式，其程式可以在Apple MAC的Intel及ARM-based環境架構中執行。2024 年 4 月 24 日，研究人員發現了一個具有間諜軟體及竊取訊息行為的惡意 Mach-O 二進位檔案，其應用程式的名稱為 “DumpMedia Spotify Music Converter” 。該惡意軟體最初在 dumpmediacom 網站下載 Spotify 時被檢測到，後來發現在也存在其他網站上的免費和付費版本。

Cuckoo 偽裝成可以將 Spotify 的音樂轉換為 MP3 的工具，安裝

應用程式後，它會開始竊取資料，包括 macOS 鑰匙圈內容、歷史瀏覽記錄、應用程式的訊息、加密貨幣錢包詳細訊息和身份驗證的憑證。Cuckoo也會取得使用者的截圖檔案、網絡攝影機的快照和WhatsApp、Telegram 等應用程式的資料。

為了獲取更多資料，它進一步要求使用者打開沒有經過驗證的簽名或開發者 ID 的應用程式，以收集主機硬體資訊並確認使用者的位置。如果使用者選擇同意後續的要求，該惡意軟體將可取得Finder、麥克風和下載檔案的權限。

雖然該攻擊活動尚未明確歸因於任何特定的攻擊組織，但研究人員發現它不會攻擊亞美尼亞、白俄羅斯共和國、哈薩克、俄羅斯和烏克蘭的設備。Cuckoo 使用 LaunchAgent 方式持續建立連線，這與 RustBucket、XLoader、JaskaGO 以及 ZuRu 等後門功能相似。

避免Cuckoo惡意軟體攻擊，建議使用者應謹慎下載應用程式，避免不受信任的來源，仔細檢查電子郵件及其附件，並使用可靠的防毒軟體和防惡意程式的解決方案。

- 資料來源：

1. New 'Cuckoo' Persistent macOS Spyware Targeting Intel and Arm Macs
2. Cuckoo Mac Malware Mimics Music Converter to Steals Passwords and Crypto

2.3 系統資安議題

2.3.1 Tinyproxy 漏洞影響全世界約 50,000 台電腦

Tinyproxy存在use-after-free安全漏洞(CVE-2023-49606)，可透過傳送特製的 HTTP 標頭導致遠端程式碼執行(RCE)，最近已釋出安全性更新。Tinyproxy 是一個輕量級的代理，可用於 HTTP 和 HTTPS 代理，其優點包括簡單、快速和佔用空間小，非常適合在小型網路環境中使用，全球約有 90,000 台主機安裝了 Tinyproxy 服務，其中仍有超過 50% 尚未修補此嚴重安全性漏洞。

Cisco Talos 研究團隊表示，該漏洞位於程式的 remove_connection_headers() 函數中，未正確處理 http header 參數，造成記憶體被釋放後，仍能被錯誤的存取。換言之，攻擊者可透過發送含有特製 http 標頭的 http request，重新利用已釋放的記憶體，進而導致遠端程式碼執行。此漏洞由 Cisco Talos 編號為 CVE-2023-49606，CVSS 評分為 9.8 分，影響版本為 1.10.0 和 1.11.1。

資安業者 Censys 指出，統計到2024年5月3日 為止，約52,000台

主機執行存在漏洞的Tinyproxy，這些受漏洞影響的主機分散在不同國家，包含美國約32,846台、韓國約18,358台、中國約7,808台、法國約5,208 台、德國約3,680台。

Cisco Talos於2023年12月22日已報告該漏洞，並發布概念驗證程式（Proof-of-Concept, PoC），他們亦表示曾提醒 Tinyproxy 的軟體維運者此安全性問題，但一直未收到回覆，也未見到任何修補程式釋出，因此2024 年 5 月 1 日公開此漏洞，5 天後，Debian Tinyproxy 的軟體維運者注意到此公告訊息，並通知 Tinyproxy 軟體維運者該問題。Tinyproxy 軟體維運者則指責 Cisco Talos 將報告發送到一個他們不再使用的電子郵件地址，並認為 Cisco Talos 只是隨意從 git log 資訊中找尋電子郵件地址，進行漏洞通報。。

Tinyproxy 軟體維運者已將修補程式發布在其Github上，建議使用 Tinyproxy 的用戶，儘快將軟體更新至 1.11.2 版本，並不要將此服務暴露於網際網路上。

- 資料來源：

1. Tinyproxy service
2. Critical Tinyproxy Flaw Opens Over 50,000 Hosts to Remote Code Execution
3. CVE-2023-49606
4. Tinyproxy HTTP Connection Headers use-after-free vulnerability

2.4 軟硬體漏洞資訊

2.4.1 Windows Print Spooler存在高風險安全漏洞

CVE 編號	CVE-2022-38028
影響產品	Microsoft Windows
解決辦法	官方已針對漏洞釋出修復更新，請參考以下網址確認修補資訊： https://msrc.microsoft.com/update-guide/advisory/CVE-2022-38028

- 內容說明：

  近期研究人員發現，特定駭客組織利用 Windows Print Spooler 服務之舊有漏洞(CVE-2022-38028)對外進行攻擊，由於該漏洞允許本機使用者提權至系統權限，且已遭駭客廣泛利用，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 20H2 for 32-bit Systems
  Windows 10 Version 20H2 for ARM64-based Systems
  Windows 10 Version 21H1 for 32-bit Systems
  Windows 10 Version 21H1 for ARM64-based Systems
  Windows 10 Version 21H1 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 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 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Windows RT 8.1
Windows Server 2012
Windows Server 2012 (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)

- 資料來源：

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://nvd.nist.gov/vuln/detail/CVE-2022-38028
3. https://msrc.microsoft.com/update-guide/advisory/CVE-2022-38028

2.4.2 Cisco Adaptive Security Appliance (ASA)與Firepower Threat Defense (FTD)軟體存在高風險安全漏洞

CVE 編號	CVE-2024-20353
影響產品	Adaptive Security Appliance(ASA) Firepower Threat Defense(FTD)
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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2#fs

- 內容說明：

  研究人員發現 Cisco Adaptive Security Appliance (ASA)與 Firepower Threat Defense (FTD)軟體存在阻斷服務(Denial of Service)漏洞(CVE-2024-20353)，未經身分鑑別之遠端攻擊者可發送惡意請求促使裝置重新載入，進而導致無法提供服務。該漏洞已遭駭客利用，請儘速確認並進行更新修補。

- 影響平台：

  Adaptive Security Appliance(ASA)
  Firepower Threat Defense(FTD)

- 資料來源：

  1. https://nvd.nist.gov/vuln/detail/CVE-2024-20353
  2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2

2.4.3 Microsoft SmartScreen Prompt存在高風險安全漏洞

CVE 編號	CVE-2024-29988
影響產品	Microsoft 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-2024-29988

- 內容說明：

  研究人員發現 Microsoft SmartScreen Prompt 存在保護機制失效(Protection Mechanism Failure)漏洞(CVE-2024-29988)，攻擊者可利用此漏洞製作惡意網路捷徑檔案，受駭者下載並點擊該檔案後，將繞過 SmartScreen 告警執行來源不明檔案之機制，使惡意程式可於受駭者未察覺之情況下背景執行。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 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 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-2024-20353
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988
3. https://www.youtube.com/watch?v=xR0dbM9oe70

2.4.4 以Chromium為基礎之瀏覽器存在安全漏洞

CVE 編號	CVE-2024-4671
影響產品	Google Chrome Microsoft Edge(Based on Chromium) Vivaldi
解決辦法	● 請更新 Google Chrome 瀏覽器至 124.0.6367.201(含)以上版本 https://support.google.com/chrome/answer/95414?hl=zh-Hant ● 請更新 Microsoft Edge 瀏覽器至 124.0.2478.105(含)以上版本 https://support.microsoft.com/zh-tw/topic/microsoft-edge-%E6%9B%B4%E6%96%B0%E8%A8%AD%E5%AE%9A-af8aaca2-1b69-4870-94fe-18822dbb7ef1 ● 請更新 Vivaldi 瀏覽器至 6.7.3329.31(含)以上版本 https://help.vivaldi.com/desktop/install-update/update-vivaldi/

- 內容說明：

  研究人員發現 Google Chrome、Microsoft Edge 及 Vivaldi 等以 Chromium 為基礎之瀏覽器存在記憶體釋放後使用(Use After Free)漏洞(CVE-2024-4671)，且已遭駭客利用，請儘速確認並進行修補。

- 影響平台：
  - Google Chrome 124.0.6367.201(不含)以下版本
  - Microsoft Edge(Based on Chromium) 124.0.2478.105(不含)以下版本
  - Vivaldi 6.7.3329.31(不含)以下版本

- 資料來源：
  1. https://nvd.nist.gov/vuln/detail/cve-2024-4671
  2. https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_9.html
  3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-4761
  4. https://vivaldi.com/blog/desktop/minor-update-five-6-7/
  5. https://support.google.com/chrome/answer/95414?hl=zh-Hant
  6. https://support.microsoft.com/zh-tw/topic/microsoft-edge-%E6%9B%B4%E6%96%B0%E8%A8%AD%E5%AE%9A-af8aac
  7. https://help.vivaldi.com/desktop/install-update/update-vivaldi/

2.4.5 Microsoft Windows MSHTML平台存在高風險安全漏洞

CVE 編號	CVE-2024-30040
影響產品	Microsoft 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-2024-30040

- 內容說明：

  研究人員發現 Microsoft Windows MSHTML 平台存在安全功能繞過(Security Feature Bypass)漏洞(CVE-2024-30040)，遠端攻擊者可藉由誘騙使用者下載與開啟惡意檔案，繞過 Microsoft 365 與 Office 之物件連結與嵌入(OLE)防護機制，進而利用此漏洞達到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：

  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 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-2024-30040
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30040
3. https://www.ithome.com.tw/news/162875

2.4.6 Microsoft Windows桌面視窗管理(DWM)核心資料庫與存在高風險安全漏洞

CVE 編號	CVE-2024-30051
影響產品	Microsoft 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-2024-30051

- 內容說明：

  研究人員發現 Microsoft Windows 桌面視窗管理(DWM)核心資料庫存在本機提權(Local Privilege Escalation)漏洞(CVE-2024-30051)，已取得本機帳號權限之攻擊者可利用此漏洞提升至 SYSTEM 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：

  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 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)

- 資料來源：

1. https://nvd.nist.gov/vuln/detail/CVE-2024-30051
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30051
3. https://www.tenable.com/blog/microsofts-may-2024-patch-tuesday-addresses-59-cves-cve-2024-30051-cve-
4. https://www.ithome.com.tw/news/162875

2.4.7 D-Link DIR-600路由器存在高風險安全漏洞

CVE 編號	CVE-2021-40655
影響產品	D-Link
解決辦法	官方已不再支援受影響產品，建議進行汰換。

- 內容說明：

  研究人員發現 D-Link DIR-600 路由器存在敏感資訊洩漏(Sensitive Information Disclosure)漏洞(CVE-2021-40655)，未經身分鑑別之遠端攻擊者可發送偽造之 POST 請求以取得使用者帳號與通行碼。該漏洞已遭駭客利用，請儘速確認並採取對應措施。

- 影響平台：

  D-Link dir-605 B2 2.01MT

- 資料來源：

  1. https://nvd.nist.gov/vuln/detail/CVE-2021-40655
  2. https://www.cvedetails.com/cve/CVE-2021-40655
  3. https://github.com/Ilovewomen/D-LINK-DIR-605

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】6/6資通系統委外開發RFP	
活動時間	**2024-06-06 13:30 ~ 2024-06-06 16:30**
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/5266**
活動概要	 **【費用】** 原價：NT 3,300 元/人 早鳥價：NT 3,000 元/人(課前一個月報名) 軟協會員價：NT 2,800 元/人 費用含稅、教材及完課證明 **【活動內容 / Event Deails】** 本課程旨在針對委外開發技術面及管理面資安需求，並依據資通系統防護基準控制措施構面，進行 SSDLC 安全的系統開發生命週期實務操作，制定資安需求項目資訊系統委外安全管理。可依據系統防護需求等級，選取適用之需求項目。 **【主辦單位】**中華民國資訊軟體協會 **【聯絡窗口】** 02-2553-3988 分機 388、816 廖資深專員、林專員 security@cisanet.org.tw **【報名截止】**2024-05-30

【資策會】6/6 工控資安(OT)教育訓練	
活動時間	**113年06月06日(四)09:00-16:30**
活動地點	**ACW SOUTH 數位產業署沙崙資安服務基地C115攻防演訓教室(臺南市歸仁區歸仁十三路一段6號)**
活動網站	**https://ievents.iii.org.tw/EventS.aspx?t=0&id=2464**
活動概要	 **【費用】** 免費 **【課程講師】**國際自動化協會臺灣分會　林上智會長 **【活動內容 / Event Deails】** ● 理解並應用 ISA/ IEC 62443 標準於日常的 OT 資安管理中。 ● 設計與執行全面的風險評估和管理計畫。 ● 建立並實施有效的資安防護和應急響應策略。 ● 促進組織內的資安意識與文化建設。 **【課程對象】**OT 系統管理者與操作者、資安負責人與技術支援人員、資產擁有者與負責人 **【主辦單位】**數位發展部數位產業署 **【執行單位】**財團法人資訊工業策進會 **【聯絡窗口】**林先生　linpinghui@iii.org.tw　02-6631-6633 **【報名截止】**2024-05-31

【資策會】6/13 SSDLC安全性軟體開發實務	
活動時間	**113年06月13日(四)09:30-16:30 (共6小時，休息1小時)**
活動地點	**ACW SOUTH 數位產業署沙崙資安服務基地C115攻防演訓教室(臺南市歸仁區歸仁十三路一段6號)**
活動網站	**https://ievents.iii.org.tw/EventS.aspx?t=0&id=2445**
活動概要	 **【費用】** 免費 **【課程講師】**叡揚資訊股份有限公司陳宇馳顧問 **【活動內容 / Event Deails】** ● 實際的做法為何。 ● 使開發團隊中的每個角色了解彼此的資安需求與做法，建立一致的資安目標，讓團隊運作更順暢。 **【課程對象】**資訊人員、網路管理人員、資安推動/應用人員 **【主辦單位】**數位發展部數位產業署 **【執行單位】**財團法人資訊工業策進會 **【聯絡窗口】**陳小姐 yuxuanchen@iii.org.tw 02-6631-6758 林小姐 tiffanylin@iii.org.tw 02-66316672 **【報名截止】**2024-05-31

【資策會】6/17 IT人員輕鬆掌握OT技術關鍵即戰力	
活動時間	113年06月17日(一)09:30-16:30 (共6小時，休息1小時)
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://ievents.iii.org.tw/EventS.aspx?t=0&id=2433
活動概要	 **【費用】** 免費 **【課程講師】**椰棗科技羅堅誌講師 **【活動內容 / Event Deails】** ● 安全之間的區別 ● 安全威脅，理解其對工業生產和基礎設施安全的潛在影響 ● 能夠選擇和安裝開源工控軟體，搭建簡易的 OT 模擬環境，進行實踐操作 **【課程對象】**資訊人員、網路管理人員、資安推動/應用人員 **【主辦單位】**數位發展部數位產業署 **【執行單位】**財團法人資訊工業策進會 **【聯絡窗口】**陳小姐 yuxuanchen@iii.org.tw 02-6631-6758 林小姐 tiffanylin@iii.org.tw 02-66316672 **【報名截止】**2024-06-03

【資安學院-國際證照班】6/20-6/21 NIST網路安全框架建置訓練課程	
活動時間	**2024-06-20 09:00 ~ 2024-06-21 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/5180**
活動概要	 **【費用】** 原價：NT 22,500 元/人 早鳥價：NT 22,000 元/人(課前兩個月報名) 軟協會員價：請洽軟協承辦人 費用含稅、教材、餐點及完課證明 **【課程講師】**BSI 台灣分公司專業合格之講師授課 **【活動內容 / Event Deails】** 熱門的零信任架構，即參考 NIST 網路安全框架。本課程您將了解如何使用 NIST 網路安全框架來幫助組織預防、偵測和回應網絡攻擊；此外還將了解如何將 NIST 網路安全框架與其他管理系統整合，特別是 ISO / IEC 27001 及附錄 A 的控制措施。課程進行方式包含講師解說，小組討論和課堂學習。 **【主辦單位】**中華民國資訊軟體協會 **【聯絡窗口】**02-2553-3988 分機 388、816　廖資深專員、林專員 security@cisanet.org.tw **【報名截止】**2024-06-13

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：

鼎新電腦 EasyFlow .NET- SQL Injection	
TVN / CVE ID	TVN-202405001 / CVE-2024-4893
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	EasyFlow .NET V3.x,V5.x,V6.1.x,V6.6.x
問題描述	鼎新電腦 EasyFlow .NET 之部分功能參數未對使用者輸入進行驗證，允許遠端攻擊者在不需權限的情況下，即可注入任意 SQL 指令讀取、修改及刪除資料庫內容，並可以執行系統指令。
解決方法	更新至 v6.6.15 (2023/12/01釋出) 或之後版本
公開日期	2024-05-15
相關連結	https://www.twcert.org.tw/tw/cp-132-7800-843f1-1.html

新夥伴科技 N-Reporter 與 N-Cloud - Os Command Injection	
TVN / CVE ID	TVN-202405004 / CVE-2024-5400
CVSS	8.8 (High) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
影響產品	Mail2000 V8.0 Patch 34(不含)以前版本
問題描述	網擎資訊 Mail2000 未妥善過濾特定CGI之參數，已取得一般權限之遠端攻擊者，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	更新 Mail2000 V8.0 至 Patch 34(含)以後版本
公開日期	2024-05-27
相關連結	**https://www.twcert.org.tw/tw/cp-132-7819-9661a-1.html**

雲端數位科技 MinMax CMS - Hidden Functionality	
TVN / CVE ID	TVN-202405006 / CVE-2024-5514
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	MinMax CMS
問題描述	雲端數位科技 MinMax CMS 存在隱藏的管理員帳號，該帳號密碼固定且無法於管理介面移除或停用，取得該帳號的遠端攻擊者，可不受IP存取控制的限制登入後台系統，且登入活動不會被系統紀錄。
解決方法	請詢問廠商取得修補建議
公開日期	2024-05-30
相關連結	**https://www.twcert.org.tw/tw/cp-132-7828-c08b8-1.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 5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/**

Twitter：**@TWCERTCC**