TWCERT/CC 資安情資電子報

2024 年 12 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、新興應用資安及資安小知識。

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

2023年最常被利用的漏洞

美國網路安全暨基礎架構管理署(Cybersecurity and Infrastructure Security Agency，CISA)與多個國際資安組織於11月12日共同發布資安公告，彙整2023年常見駭客利用47個漏洞資訊與修補方式。

2023年最常利用的47個漏洞涉及廠商共有28家(綜整如表1)。其中以Microsoft因其中5個漏洞被頻繁利用，成為受影響最嚴重的公司之一；2023年在這些漏洞中，影響最廣的前四大漏洞分別來自 Citrix 和 Cisco。其中，Citrix 的兩個漏洞 CVE-2023-3519 和 CVE-2023-4966，以及 Cisco 的兩個漏洞 CVE-2023-20198 和 CVE-2023-20273，成為攻擊者的主要目標，對全球資訊安全環境帶來重大挑戰。

Citrix 旗下產品NetScaler Gateway是一款提供使用者遠端訪問應用程式和數據的控制平台；NetScaler ADC是負責平台交付和負載平衡解決方案。2023年最常被利用的前二名漏洞CVE-2023-3519 (CVSS 3.x：9.8) 和 CVE-2023-4966 (CVSS 3.x：9.4)，均影響Citrix NetScaler Gateway和NetScaler ADC。CVE-2023-3519 允許未經身分驗證的使用者透過發送HTTP GET請求，導致NSPPE程序發生緩衝區溢出；而CVE-2023-4966則可能導致Session Token洩漏。

第三名與第四名則是影響Cisco為網路裝置所開發的維護作業系統Cisco IOS XE漏洞，分別為CVE-2023-20198 (CVSS 3.x：10.0) 和 CVE-2023-20273 (CVSS 3.x：7.2)，這兩個漏洞皆存在於Cisco IOS XE的Web UI，CVE-2023-20198允許未經授權的使用者獲得最初訪問權限，並建立本地使用者帳號和密碼，從而以一般使用者身分登入系統。CVE-2023-20273是一個命令注入漏洞，同樣存在於Cisco IOS XE的Web UI，與CVE-2023-20198相關，駭客可利用最高權限將惡意程式寫入檔案系統，進而控制整個系統。

建議企業與使用者儘速檢視系統，確保所有相關漏洞已被適當修補，以降低風險，更多漏洞資訊可至CISA官方網站查看2023 Top Routinely Exploited Vulnerabilities。

表1、2023年最常利用的47個漏洞

項次	廠商	CVE 編號
1	Apache	CVE-2021- 44228
2	Apple	CVE-2023-41064、CVE-2023-41061
3	Atlassian	CVE-2023-22515、CVE-2023-22518、CVE-2021-26084、CVE-2022-26134
4	Barracuda Networks	CVE-2023-2868
5	Cisco	CVE-2023-20198、CVE-2023-20273、CVE-2017-6742

6	Citrix	CVE-2023-3519、CVE-2023-4966
7	Dahua	CVE-2021-33044、CVE-2021-33045
8	F5	CVE-2021-22986
9	FatPipe	CVE-2021-27860
10	Fortinet	CVE-2023-27997、CVE-2018-13379
11	Fortra	CVE-2023-0669
12	GitLab	CVE-2021-22205
13	Ivanti	CVE-2023-35078、CVE-2023-35081、CVE-2019-11510
14	JetBrains	CVE-2023-42793
15	Juniper	CVE-2023-36844、CVE-2023-36845、CVE-2023-36846、CVE-2023-36847
16	Microsoft	CVE-2020-1472、CVE-2023-23397、CVE-2019-0708、CVE-2022-41040、CVE-2021-34473
17	Netwrix	CVE-2022-31199
18	Novi	CVE-2023-29492
19	ownCloud	CVE-2023-49103
20	PaperCut	CVE-2023-27350
21	Progress	CVE-2023-34362
22	Progress Telerik	CVE-2019-18935
23	RARLAB	CVE-2023-38831
24	Red Hat	CVE-2021-4034
25	Sophos	CVE-2022-3236
26	Unitronics	CVE-2023-6448
27	Zoho	CVE-2022-47966、CVE-2021-40539
28	N/A	CVE-2023-44487

- 相關連結

1. CISA-2023 Top Routinely Exploited Vulnerabilities
2. NIST NVD - CVE-2023-3519
3. NIST NVD – CVE-2023-4966
4. NIST NVD – CVE-2023-20198
5. NIST NVD – CVE-2023-20273

第 2 章、國內外重要資安事件

2.1 新興應用資安

2.1.1 Venom Spider利用 MaaS平台部署的新型惡意程式

提供各種MaaS工具聞名的駭客組織Venom Spider (又稱Golden Chickens) 在2024年8月至10月期間，發現兩個惡意程式RevC2 和 Venom Loader使用其 MaaS工具進行部署。根據Zscaler的研究報告指出，這可能是新一代惡意程式家族的早期版本，未來有可能升級為更複雜的攻擊行動。

MaaS (Malware-as-a-Service) 是一種將惡意程式商品化的模式，駭客無需自行編寫或編譯惡意程式，而是直接訂購其他駭客開發的攻擊工具包，這種營運模式大幅降低發動網路攻擊的門檻，擴大網路安全威脅的範圍。

第一次的攻擊行動在2024年8月至9月，攻擊手法由VenomLNK檔案開始，此LNK檔包含一個混淆的批次(BAT)腳本，當腳本啟動

後，會執行一張含有API檔案內容的圖片，利用該API文件作為誘餌，傳遞並執行能夠竊取敏感資料的RevC2後門程式，RevC2再透過WebSocket與C2進行通訊，其C2位置為ws://208.85.17[.]52:8082。

ThreatLabz開發模擬RevC2的Python腳本，供使用者測試設備是否有相關受害跡象，該腳本已上傳至ThreatLabz的Github儲存庫中，網址為：hxxps://github[.]com/ThreatLabz/tools/tree/main/revc2。

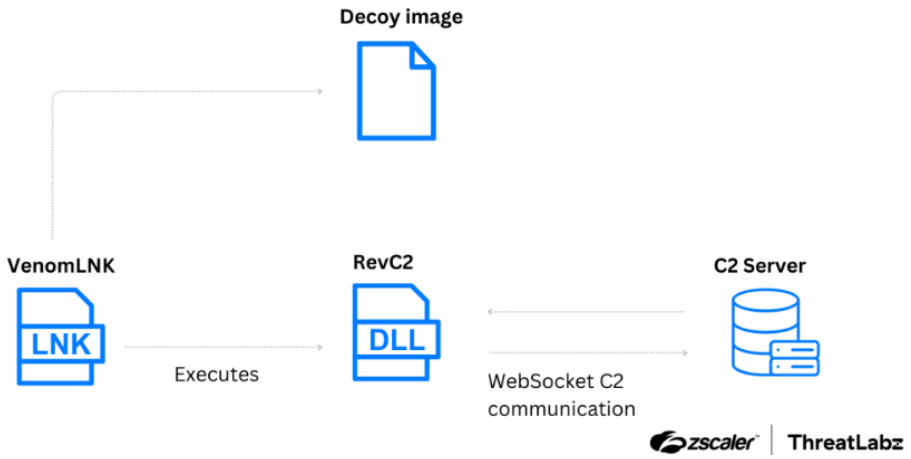

圖1:以RevC2作為有效負載的攻擊鏈。圖片來源：Zscaler Blog

Zscaler ThreatLabz 研究人員觀察到第二次的攻擊行動則在2024年9月至10月期間進行，其攻擊手法與第一次相似，但此次攻擊以虛擬貨幣交易為誘餌，傳遞惡意程式Venom Loader並載入以JavaScript編譯的後門程式More_eggs lite，此後門程式含有遠端程式碼執行的功能。

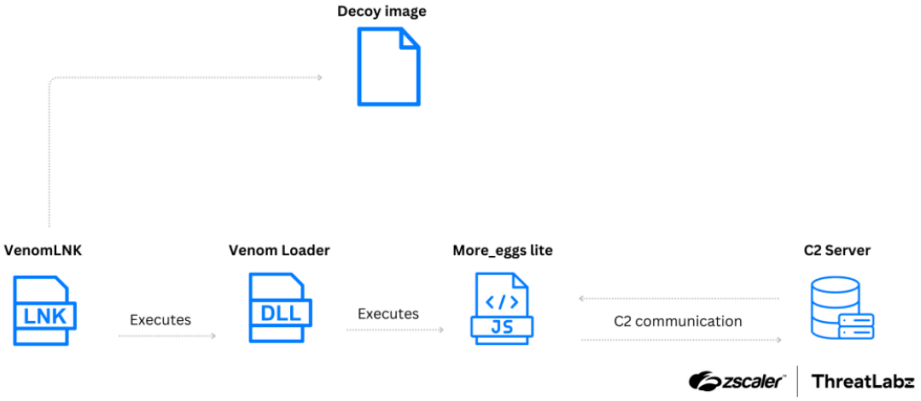

圖2:以More_eggs lite作為有效負載的攻擊鏈。圖片來源：Zscaler Blog

利用MaaS所提供的工具進行網路攻擊日益增多，技術也不斷進化，民眾和企業應提高警覺，防範惡意程式、定期檢查系統安全，對抗網路威脅。

- 資料來源：

1. Venom Spider Spins Web of New Malware for MaaS Platform
2. Unveiling RevC2 and Venom Loader
3. ThreatLabz –模擬 RecC2的Python腳本
4. More_eggs MaaS Expands Operations with RevC2 Backdoor and Venom Loader

2.2 資安趨勢

2.2.1 2025年資安趨勢與供應鏈安全挑戰

隨著科技的持續發展與全球數位化的加速，資訊安全的重要性日益增加。人工智慧、大數據、物聯網等技術的普及應用，使得網路攻擊的範圍和形式變得更加複雜和多樣化。對企業而言，不僅是技術上的挑戰，更涉及到業務營運、品牌信譽等多方面的風險。

根據趨勢科技發布《2025年資安年度預測報告》，報告內容指出，隨著資安威脅持續演變，未來供應鏈可能面臨AI攻擊、國家級駭客集團對雲端環境攻擊。

當企業將代理式AI應用於業務的自動化工具，由於操作人員無法直接掌握事件互動的細節，進而導致企業資安帶來隱憂。例如與大型語言模型(LLM)進行互動時，可能會無意中洩露敏感資料，包括個人識別資訊、智慧財產權、公司機密等。

此外，趨勢科技預測國際政治局勢的變化，國家級駭客集團如Lazarus、Turla和Pawn Storm等，預計在2025年繼續活躍並加強攻擊。

面對駭客不斷開發新漏洞並進行入侵，企業必須了解自身在供應鏈中的角色，並建立多層次的防禦措施，採取風險管理策略保護關鍵基礎設施和資訊安全，這不僅關乎產品的流通，更涉及到資訊安全的整體防護。

另外，勒索病毒的攻擊策略也正發生變化，也是企業必須關注另一項重要議題。趨勢科技針對台灣服務案件進行統計，2024年約九成的目標式勒索攻擊事件針對中小企業，顯示中小企業因資源有限，而成為駭客的主要攻擊目標，因此更加需要加強資安防護措施。

總體而言，2025年資安趨勢顯示，供應鏈安全的重要性不斷上升，而AI技術將在網路犯罪中扮演著愈加關鍵的角色。無論企業大小，都應加強風險管理策略，保護自身及供應鏈免受潛在威脅。同時，提升員工對資安意識的教育，也是防範攻擊的重要一環。

- 資料來源：

1. 趨勢科技 – 資安報告與年度預測
2. NCSC - Supply Chain Cyber Security
3. NIST – Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

2.3 行動裝置資安訊息

2.3.1 揭露！中國警方操控的 Android 間諜軟體曝光

資安公司 Lookout 近期發現一款名為 EagleMsgSpy的Android 間諜軟體，並認為該軟體由中國操控，主要用於監控使用者的手機。這款間諜軟體能從 Android手機中竊取大量資料，包含通訊訊息、螢幕錄影、通話記錄等。目前尚未發現iOS系統的版本。

根據上傳至 VirusTotal的版本資料顯示，該間諜軟體自2017年起已被使用，至今仍持續開發與演變，存在多個變種。Lookout 資安團隊表示，目前在Google Play商店或其他應用程式商店並未觀察到此惡意程式的存在。

Lookout分析報告指出，此款間諜軟體似乎是由一個軟體開發商提供給多個客戶使用，因為要求使用者輸入特定的頻道(channel)，每個頻道對應一位使用者。透過歷史樣本的分析，資安專家發現該惡意程式在加密金鑰的混淆和儲存方式上不斷變化，顯示開發者對隱蔽性和抗分析能力的重視，證實該惡意程式正積極維護。

該間諜軟體主要目的為竊取Android手機上面的資料，包含通訊

軟體的訊息(QQ、Telegram、Viber、WhatsApp、微信)、監控螢幕畫面、通話紀錄、簡訊、聯絡人資訊、GPS座標位置、無線網路資訊、瀏覽器書籤等。資料被竊取後，首先存放於設備檔案系統中的隱藏資料夾，再壓縮並加密傳送至惡意中繼站。

圖3: Lookout 研究人員發現針對此間諜軟體的說明文件，內容包含安裝設備和使用。

追蹤EagleMsgSpy的過程中，Lookout研究人員發現惡意中繼站所使用的IP位置曾與武漢中企軟通科技有限公司的子網域有關聯，後續調查該中國企業使用的根網域為tzsafe.com，其中字串tzsafe是間諜軟體的監控模組密碼，因此分析人員認為此間諜軟體是由武漢中企軟通科技有限公司所開發和維護。

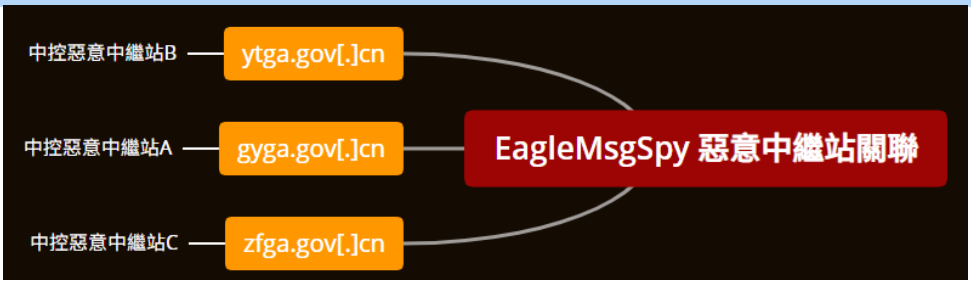

圖4:是整理Lookout研究人員發現該間諜軟體所使用的惡意中繼站之關聯圖。

使用者應提高警覺，除安裝可靠的防毒軟體並定期掃描手機外，保持系統和應用程式的最新版本。此外，應從官方網站下載應用程式，提高對網路釣魚攻擊的敏感度。這些措施能顯著降低資料被竊取的風險，保護個人隱私與安全。

- 資料來源：

1. Lookout Discovers New Chinese Surveillance Tool Used by Public Security Bureaus

2.4 軟硬體漏洞資訊

2.4.1 Apache Struts 2存在安全漏洞

CVE 編號	CVE-2024-53677
影響產品	Apache struts 2
解決辦法	官方已針對漏洞釋出修復更新，請參考官方說明，網址如下： https://cwiki.apache.org/confluence/display/WW/S2-067

- 內容說明：

  研究人員發現 Apache struts 2 存在任意檔案上傳(Arbitrary File Upload)漏洞(CVE-2024-53677)，允許未經身分鑑別之遠端攻擊者上傳網頁後門程式並於伺服器端執行，請儘速確認並進行修補。

- 影響平台：
  - Struts 2.0.0 至 2.3.37 版本
  - Struts 2.5.0 至 2.5.33 版本
  - Struts6.0.0 至 6.3.0.2 版本
- 資料來源：

  1. https://nvd.nist.gov/vuln/detail/CVE-2024-53677
  2. https://cwiki.apache.org/confluence/display/WW/S2-067
  3. https://www.ithome.com.tw/news/166558

2.4.2 微軟通用紀錄檔系統(CLFS)驅動程式存在安全漏洞

CVE 編號	CVE-2024-49138
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，網址如下：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138

- 內容說明：

  研究人員發現微軟通用紀錄檔系統(Common Log File System, CLFS)驅動程式存在權限提升(Elevation of Privilege)漏洞(CVE-2024-49138)，允許已取得系統一般權限之本機端攻擊者進一步取得系統(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 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 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 11 Version 24H2 for ARM64-based Systems
  - Windows 11 Version 24H2 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 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- 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)
- Windows Server 2022, 23H2 Edition (Server Core installation)
- Windows Server 2025
- Windows Server 2025 (Server Core installation)

- 資料來源：

1. https://nvd.nist.gov/vuln/detail/CVE-2024-49138
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138
3. https://www.ithome.com.tw/news/166452

2.4.3 WordPress外掛Really Simple Security存在安全漏洞

CVE 編號	CVE-2024-10924
影響產品	WordPress
解決辦法	官方已針對漏洞釋出修復更新，請更新至以下版本： WordPress 外掛 Really Simple Security 9.1.2(含)以後版本

- 研究人員內容說明：

  WordPress 外掛 Really Simple Security 存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2024-10924)，在雙因子認證功能啟用狀態下，未經身分鑑別之遠端攻擊者可用任意使用者身分登入系統，請儘速確認並進行修補。

- 影響平台：
  - WordPress 外掛 Really Simple Security 9.0.0 至 9.1.1.1 版本
- 資料來源：
  1. https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=11388
  2. https://nvd.nist.gov/vuln/detail/CVE-2024-10924

第 3 章、資安研討會及活動

- **資安研討會**

【資安院】1月線上攻防平台實作課程	
活動時間	**114/1/22(三)下午2-4點**
活動地點	**線上方式進行**
活動網站	**https://www.facebook.com/te.nics.tw**
活動概要	 **【費用】** 免費 報名截止： **114/1/2(四)上午 10:00 - 113/1/3(五)下午 6:00** **【課程目的】** 提供資安攻防專題演訓實作課程，訓練學習者了解攻擊思維，並掌握防禦技能。 **【訓練時間】** 114 年 1 月 22 日（星期三）下午 2-4 時 **【訓練地點】**

	採線上授課及演練操作，授課及演練連結網址另行提供。 **【報名方式】** 1.報名連結將於 1/2(四)上午 10:00 公告於 FB 資安人蔘粉絲專頁、資安院官網，敬請留意！ 2.資安人蔘 https://www.facebook.com/te.nics.tw 3.資安院官網 https://www.nics.nat.gov.tw/latest_news/announcements/Event_Information/

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：

中華電信 文件傳輸程式 - Reflected Cross-site Scripting to RCE	
TVN / CVE ID	TVN-202412001 / CVE-2024-12641
CVSS	9.6 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
影響產品	文件傳輸程式 0.41.151 至 0.41.156 版本
問題描述	中華電信文件傳輸程式存在 Reflected Cross-site Scripting漏洞。該程式會架設簡易本機端網站並提供API與標的網站溝通，由於API未對CSRF做防護，未經身分鑑別之遠端攻擊者可利用釣魚的方式使用特定API於使用者瀏覽器執行任意JavaScript程式碼。因該程式架設之網站支援Node.Js特性，攻擊者可進一步利用達到執行任意作業系統指令。
解決方法	更新至0.41.157(含)以後版本
公開日期	2024-12-16
相關連結	**https://www.twcert.org.tw/tw/cp-132-8292-4fd98-1.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12月31 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/**