# TWCERT/CC 資安情資電子報

## 2024 年 10 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

# 第 1 章、封面故事

## 首個透過聊天機器人生成的惡意程式在野外散播


HP Wolf Security 的資安研究人員在今年6月的事件調查中，揭露了一項新興的攻擊手法。調查顯示，駭客運用人工智慧聊天機器人生成 VBScript 和 JavaScript 的惡意腳本，並通過這些腳本成功傳播名為 AsyncRAT 的惡意程式。此次調查的起始點是一封來自法國的可疑電子郵件，該郵件引起了資安人員的高度關注。

AsyncRAT 是一種開源的遠端存取工具，可透過安全加密連線遠端監視，並控制他人的電腦，由於擁有鍵盤紀錄器、遠端桌面控制等多種對受害者電腦造成損害的功能，因此經常被利用做為攻擊鏈的最後環節。該工具可以透過各種方式傳播，例如魚叉式網路釣魚、惡意廣告、漏洞利用工具包等。

圖 1 為此次事件的攻擊鏈，首先，駭客透過釣魚信件夾帶一個HTML檔案，當受害者開啟HTML檔案時，即觸發由VBScript寫的惡意腳本，該腳本將惡意程式相關的資料寫入註冊表，並在受駭者的資料夾中創建一個JavaScript腳本。接者，透過工作排程實現持久化並執行JavaScript惡意腳本。JavaScript 腳本會讀取先前寫入註冊表的資料，以執行Powershell腳本內容，最後，Powershell腳本會解碼在註冊表中的資料，獲取最終駭客想要執行的惡意程式AsyncRAT。

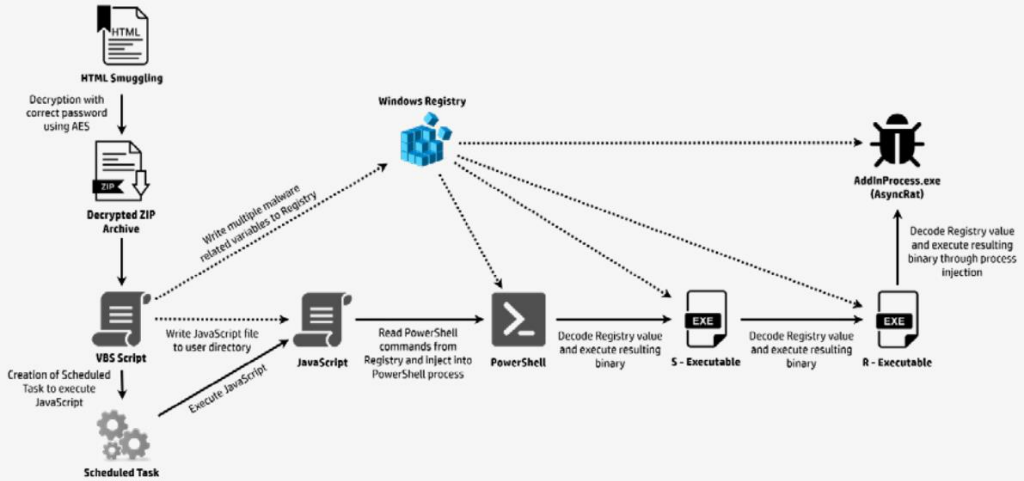



圖1: GenAI 產生惡意程式散播 AsyncRAT，圖片取自HP Wolf Security研究報告

資安研究人員認為此次事件中，圖1的VBScript和JavaScript惡意腳本可能是透過AI生成。一般來說，惡意程式會儘可能混淆使分析更加困難，但是，這次事件中的VBScript和JavaScript惡意腳本，不僅沒有進行混淆，還包含大量的註解。圖2為此次事件的VBScript惡意腳本內容，大量的註解似乎是為了要讓AI 聊天機器人能夠理解其需求。

```
// Arrête un processus PowerShell en cours d'exécution
function arreterProcessusAvecPowerShell() {
    // Exécution de PowerShell
    shellWsh.Run(cheminPowerShell, 2);

    // Obtenir la collection des processus en cours via WMI
    var serviceWMI = obtenirServiceWMI();
    var requeteProcessus = "SELECT * FROM Win32_Process";
    var collectionProcessus = serviceWMI.ExecQuery(requeteProcessus);
    var enumerateur = new Enumerator(collectionProcessus);

    // Parcours des processus en cours
    for (; !enumerateur.atEnd(); enumerateur.moveNext()) {
        var processus = enumerateur.item();

        // Si le processus en cours est PowerShell
        if (processus.Name.toLowerCase() === "powershell.exe") {
            // Activation de la fenêtre PowerShell
            shellWsh.AppActivate(processus.ProcessId);

            // Envoi de commandes pour arrêter le processus conhost
            envoyerCommandesPourArreterConhost();

            // Pause pour permettre l'arrêt du processus
            WScript.Sleep(5000);
            break;
        }
    }
}
```

圖2: VBScript 惡意腳本內容，圖片取自HP Wolf Security研究報告

隨著人工智慧的發展，人們普遍認為駭客可以利用AI撰寫惡意程式，但目前幾乎沒有實質證據顯示由AI生成的惡意程式在實際環境中散播。然而，這次的駭客攻擊提供充分的證據，展示人工智慧如何加速駭客進行惡意攻擊，降低駭客感染電腦需要的技術門檻。

從防禦的角度而言，攻擊者開始使用AI開發惡意程式，企業應該將AI整合至防禦體系，以識別由AI生成的威脅，同時簡化防禦人員的工作負擔，這樣不僅可以提升企業的整體安全性，還能更有效應對不斷演變的攻擊手法。

- 資料來源：
  1. GenAI Writes Malicious Code to Spread AsyncRAT
  2. HP Wolf Security - Threat Insights Report 2024.09

# 第 2 章、國內外重要資安事件

## 2.1 新興應用資安

### 2.1.1 Gophish被利用成為網路釣魚攻擊工具


思科Talos的研究人員近日發現，未知的威脅者正在利用Gophish框架發起網路釣魚攻擊，並散播兩種惡意軟體：DarkCrystal RAT（簡稱DCRat）以及一種尚未記錄的遠端存取木馬PowerRAT。

Gophish是一個開源的釣魚攻擊框架，旨在幫助組織測試其防禦釣魚攻擊的能力，該工具提供簡便的電子郵件模板，使用者可以輕鬆發送和追蹤電子郵件活動。

根據研究，此一攻擊活動主要透過兩種媒介展開：一是基於惡意的Word文檔，另一則是包含惡意JavaScript的HTML文件。受害者在攻擊過程中需要主動介入，以便在其設備上下載並啟用PowerRAT或DCRat，從而進一步威脅其資訊安全。

此次攻擊活動的主要特徵包括：

- 攻擊者可存取受害者的遠端控制，執行任意命令、管理文件和監

視使用者行為。

- 攻擊者可以在受害者的設備上，下載並執行其他檔案。
- 透過竊取插件模組，RAT可以從受害者電腦中竊取憑證、文件及財務資訊，並截取螢幕截圖與記錄鍵盤操作。
- RAT會在ProgramData、Pictures、Saved Games 和Windows 開始功能表等資料夾中建立多個偽裝為合法Windows執行檔案的二進位檔案，如csrss.exe、dllhost.exe、taskhostw.exe 和winlogon.exe。也會使用隨機檔案名稱和".log" 副檔名來隱藏自己的存在。

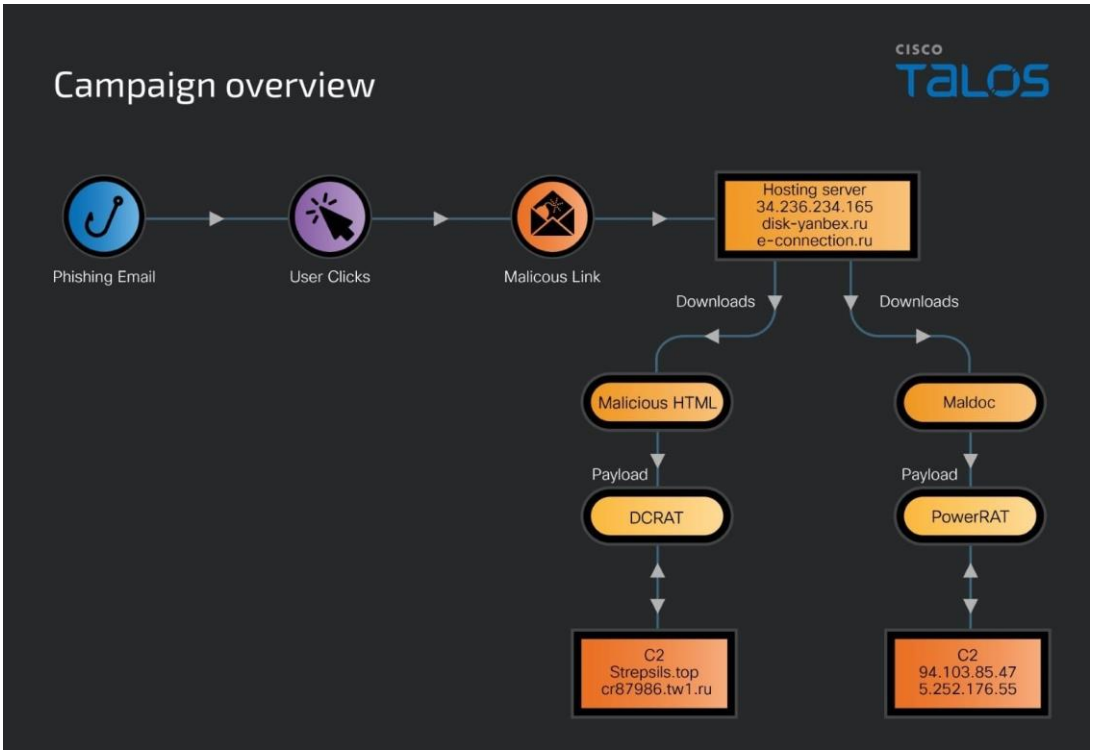



圖3. 釣魚攻擊總覽，圖片來源於Cisco Talos研究報告

PowerRAT的攻擊手法流程如圖4所示，當受害者開啟惡意檔案並啟用巨集時，惡意巨集會擷取HTML應用程式檔案和PowerShell載入程式，HTML應用程式隨後刪除負責執行PowerShell載入程式的 JavaScript 檔案，並利用合法Windows二進位檔案執行。該惡意檔案可以進行系統偵查、收集驅動器序列號，並連接至位於俄羅斯

的遠端伺服器以接收進一步指令。

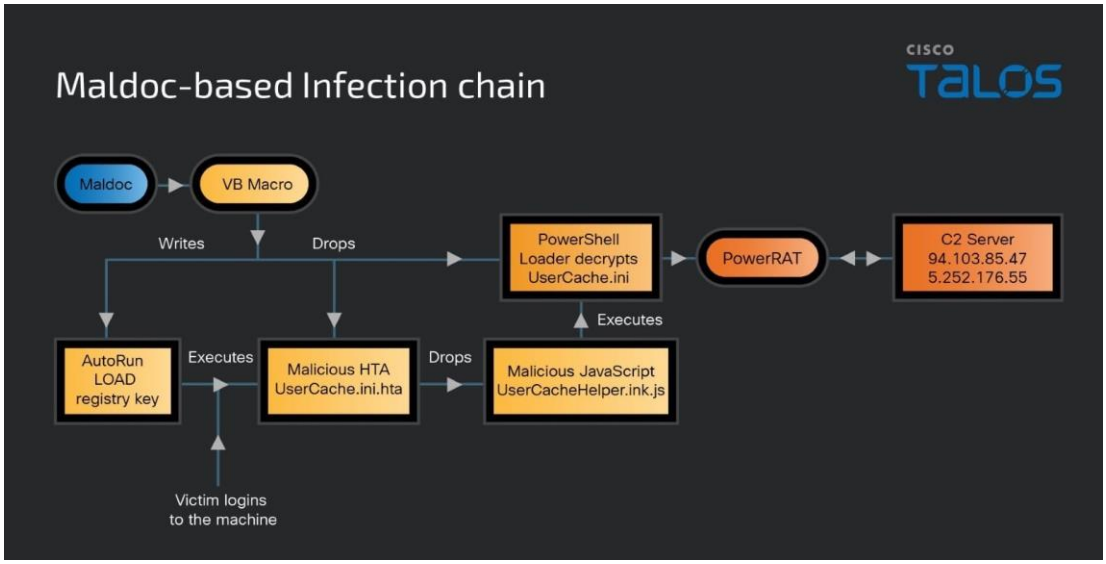



圖4. 基於Maldoc感染產生的PowerRAT，圖片來源於Cisco Talos研究報告

此外，攻擊者在此次活動還包含DCRAT的攻擊手法流程如圖5所示，使用嵌入惡意JavaScript的HTML文件，透過釣魚郵件發送給受害者，當受害者點擊釣魚郵件中的鏈接時，包含惡意JavaScript的遠端HTML文件，會在受害者的電腦瀏覽器打開，並執行多步驟的過程，最終下載並執行DCRAT，其中JavaScript中包含惡意SFX RAR可執行的7-Zip壓縮檔。

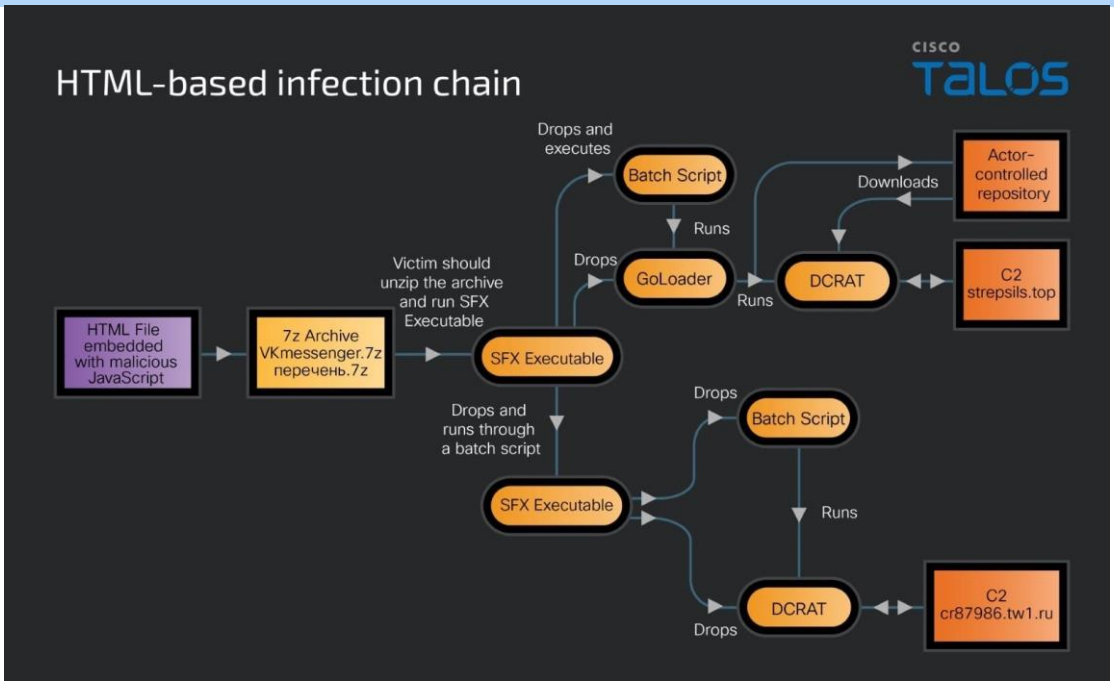


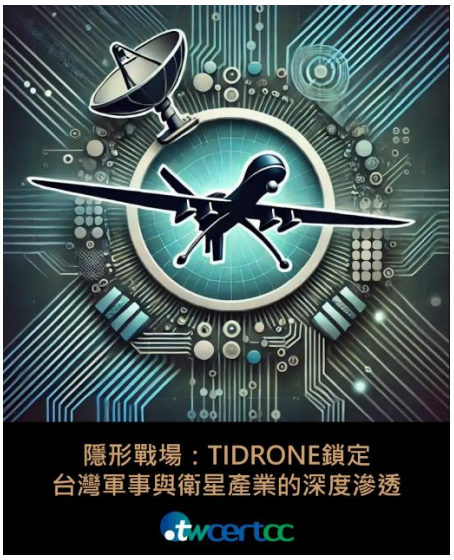

圖5. 基於HTML感染產生的DCRAT，圖片來源於Cisco Talos研究報告

使用者在處理不明來源的電子郵件時，應保持高度警惕，切勿隨意點擊來路不明的連結或是附件，防止成為這些複雜攻擊的受害者，企業和個人也應加強對釣魚攻擊的防範措施，並保持對新興威脅的關注。

- 資料來源：
  1. Gophish Framework Used in Phishing Campaigns to Deploy Remote Access Trojans
  2. Threat actor abuses Gophish to deliver new PowerRAT and DCRAT

## 2.2 資安趨勢

### 2.2.1 隱形戰場：TIDRONE鎖定台灣軍事與衛星產業深度滲透




TIDRONE是趨勢科技於2024年發現並命名的APT組織，該組織針對台灣的軍事和衛星產業發動精密的網絡攻擊，特別集中於無人機製造商。趨勢科技目前推測，此APT組織可能與中國有關，並擁有兩個專屬惡意程式，CXCLNT主要用於竊取受害者的電腦資訊，而CLNTEND則是一種遠端存取木馬，支援五種協定以與惡意中繼站進行溝通，協定分別為TCP、HTTP、HTTPS、TLS和SMB。

TIDRONE主要的入侵方式為以下兩種：

- 利用UltraVNC遠端桌面存取軟體下載惡意程式。
- 滲透ERP系統進行攻擊。(趨勢科技的分析報告指出，受害者均使用相同的 ERP 系統)

程式執行的流程與以往的中國APT組織相似，均透過執行器(Launcher)進行DDL側載(Dll-SideLoading)的方式，載入惡意載入器(Loader)。接著，解密已加密的惡意負載(payload)，獲取最終的惡意

程式。

趨勢科技透過VirusTotal分析上傳的惡意程式，發現受害地區遍及韓國、加拿大及台灣，如圖 1 所示。這顯示攻擊者針對的目標地區各不相同，因此各國應對此威脅保持警惕。

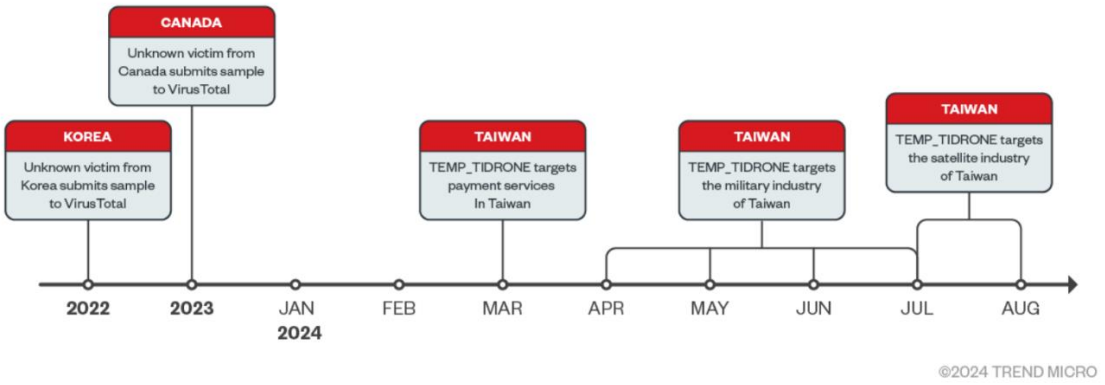



圖1：圖為 2024 年從 VT 獲取的受害者來源整理，取自趨勢科技文章

趨勢科技表示，針對攻擊者使用的惡意中繼站名稱，觀察到該組織傾向於利用正規公司的名稱來誤導使用者點擊，例如此次攻擊使用的惡意中繼站包括 symantecsecuritycloud[.]com 、microsoftsvc[.]com 和 windowswns[.]com，這三個名稱均仿照常見的公司名 Symantec, microsoft, windows。

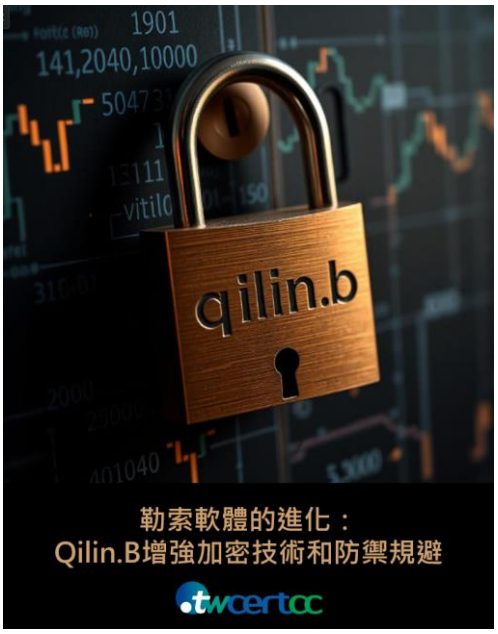
建議企業和使用者採取以下的措施進行防護：

- 從可信賴的來源端下載軟體。
- 對社交工程保持高度警惕。
- 安裝防毒軟體並保持系統更新至最新版。

- 資料來源：

1. TIDRONE Targets Military and Satellite Industries in Taiwan
2. 'TIDrone' Cyberattackers Target Taiwan's Drone Manufacturers

## 2.2.2 勒索軟體的進化：Qilin.B增強加密技術和防禦規避




資安公司Halcyon近日追蹤到一種名為Qilin.B的進階勒索軟體版本，該版本是自2022年7月首次出現的Qilin（又名Agenda）勒索軟體的最新變種。Qilin.B專門針對Windows和Linux系統進行攻擊，並透過竊取資料實施雙重勒索。

根據Halcyon的報告，Qilin.B在加密複雜性和規避技術上有顯著提升。此版本的勒索軟體使用AES-256-CTR加密算法，適用於支持AESNI的系統，同時對於不支持AESNI的系統則採用Chacha20加密。此外，為了保護加密密鑰，Qilin.B還使用了RSA-4096與OAEP填充技術，使得在沒有攻擊者私鑰或捕獲的種子值(Seed)的情況下，幾乎無法解密文件。

以下是Qilin.B的特點：

- Qilin.B結合AES-256-CTR加密技術，支持AESNI系統，同時對其他系統保留Chacha20，並使用RSA-4096和OAEP保護加密密鑰，使得沒有私鑰的情況下無法解密文件。

- Qilin.B使用Rust編譯，能終止或停用安全工具、備份和虛擬化相關的服務，如Veeam、VSS、SQL、Sophos、Acronisagent和SAP。
- 持續清除Windows事件日誌以阻礙取證分析，導致檢測和逆向工程分析變得更加困難。

Qilin.B根據系統支援不同的加密技術，如AES-256-CTR或Chacha20，將一個可配置字串附加到加密檔案中，該字串同時作為識別和追蹤的company_id。當受害者遭受攻擊時，Qilin.B會生成名為「README-RECOVER-[company_id].txt」的勒索文件，裡面包含付款詳情和解密指示。

Qilin最初是以Golang編寫，但後來轉向以抵禦逆向工程能力而聞名的Rust編程語言。這一轉變使得Qilin.B在檢測和分析上變得更加困難。該勒索軟體還具備追蹤和識別特定目標的能力，並且能夠有效地終止安全工具相關服務、清除Windows事件日誌，甚至在完成任務後自我刪除，以減少取證痕跡。

Halcyon強調，Qilin.B的出現標誌著勒索軟體家族的進一步演化，其增強的加密機制和有效的防禦規避策略使其成為一個特別危險的威脅。隨著這類攻擊手法的不斷進化，各行各業需要提高警惕，加強資安防護措施，以防止成為下一個受害者。

由本文的案例可知，勒索軟體組織不斷演變策略，攻擊手法也日益複雜，我們需要保持警惕、密切觀察趨勢和攻擊手法，以有效應對和防範勒索軟體的威脅。

- 資料來源：

1. New Qilin.B Ransomware Variant Emerges with Improved Encryption and Evasion Tactics
2. New Qilin.B Ransomware Variant Boasts Enhanced Encryption and Defense Evasion
3. New Qilin ransomware encryptor features stronger encryption, evasion

## 2.3 軟硬體漏洞資訊

### 2.3.1 CUPS存在安全漏洞

| | |
|---|---|
| **CVE 編號** | CVE-2024-47076、CVE-2024-47175、CVE-2024-47176 及 CVE-2024-47177 |
| **影響產品** | Unix |
| **解決辦法** | 部分 Unix 作業系統已逐步釋出更新，以下列舉常見作業系統之官方修補資訊：<br>Ubuntu：<br>https://ubuntu.com/blog/cups-remote-code-execution-vulnerability-fix-available<br>Debian：<br>https://security-tracker.debian.org/tracker/CVE-2024-47076<br>https://security-tracker.debian.org/tracker/CVE-2024-47175<br>https://security-tracker.debian.org/tracker/CVE-2024-47176<br>https://security-tracker.debian.org/tracker/CVE-2024-47177<br>Red hat：<br>https://access.redhat.com/security/vulnerabilities/RHSB-2024-002<br>Fedora：<br>https://bodhi.fedoraproject.org/updates/FEDORA-2024-01127974ec<br>Open SUSE：<br>https://www.suse.com/security/cve/CVE-2024-47076.html<br>https://www.suse.com/security/cve/CVE-2024-47175.html<br>https://www.suse.com/security/cve/CVE-2024-47176.html<br>https://www.suse.com/security/cve/CVE-2024-47177.html<br>若使用之作業系統尚未釋出更新，可參考以下文章進行緩解措施：<br>https://sredevops.org/en/how-to-fix-the-critical-9-9-cve-linux-vulnerability-in-cups-a-step-by-step-guide/ |

- 內容說明：

  近期研究人員發現 Unix 通用列印系統(Common UNIX Printing System，CUPS)存在一系列安全漏洞(CVE-2024-47076、CVE-2024-47175、CVE-2024-47176 及 CVE-2024-47177)，未經身分鑑別之遠端攻擊者，可利用漏洞於受影響之 Unix 作業系統執行任意程式碼，請儘速確認並進行修補或採取緩解措施。

- 影響平台：
  - cups-browsed 2.0.1(含)以前版本
  - cups-filters 2.0.1(含)以前版本
  - libcupsfilters 2.1b1(含)以前版本
  - libppd 2.1b1(含)以前版本

- 資料來源：

1. https://nvd.nist.gov/vuln/detail/CVE-2024-47076
2. https://nvd.nist.gov/vuln/detail/CVE-2024-47175
3. https://nvd.nist.gov/vuln/detail/CVE-2024-47176
4. https://nvd.nist.gov/vuln/detail/CVE-2024-47177
5. https://jfrog.com/blog/cups-attack-zero-day-vulnerability-all-you-need-to-know/
6. https://www.ithome.com.tw/news/165257
7. https://sredevops.org/en/how-to-fix-the-critical-9-9-cve-linux-vulnerability-in-cups-a-step-by-step-guide/

## 2.3.2 Fortinet FortiManager產品存在重大資安漏洞

| | |
|---|---|
| **CVE 編號** | CVE-2024-47575 |
| **影響產品** | FortiManager |
| **解決辦法** | 對應產品升級至以下版本(或更高)<br>FortiManager 7.6.1<br>FortiManager 7.4.5<br>FortiManager 7.2.8<br>FortiManager 7.0.13<br>FortiManager 6.4.15<br>FortiManager 6.2.13<br>FortiManager Cloud 7.4.5<br>FortiManager Cloud 7.2.8<br>FortiManager Cloud 7.0.13<br>FortiManager Cloud 6.4 請遷移至固定版本 |

- 內容說明：

  FortiManager 是 Fortinet 旗下的一款具有多功能網路安全管理產品，提供單一管理介面、集中管理和監控網路等。日前，官方公開揭露一個重大資安漏洞(CVE-2024-47575，CVSS：9.8)，該漏洞發生原因於 FortiManager 的 fgfmd 常駐程式中，缺失關鍵功能漏洞[CWE-306]，未經身分鑑別之遠端攻擊者可利用特製封包於受影響產品執行任意程式碼。該漏洞已遭駭客利用，請儘速確認並進行修補。官方也提供 IoC 協助資安管理人員偵測 FortiManager 伺服器是否因漏洞而遭到破壞，詳見於參考資訊網址。

- 影響平台：
  - FortiManager 7.6.0
  - FortiManager 7.4.0 至 7.4.4
  - FortiManager 7.2.0 至 7.2.7

- FortiManager 7.0.0 至 7.0.12
- FortiManager 6.4.0 至 6.4.14
- FortiManager 6.2.0 至 6.2.12
- FortiManager Cloud 7.4.1 至 7.4.4
- FortiManager Cloud 7.2.1 至 7.2.7
- FortiManager Cloud 7.0.1 至 7.0.12
- FortiManager Cloud 6.4.0 所有版本

- 資料來源：
  1. https://nvd.nist.gov/vuln/detail/CVE-2024-47575
  2. https://www.fortiguard.com/psirt/FG-IR-24-423

# 第 3 章、資安研討會及活動

- **資安研討會**

| 【資安院】11/2~3、11/9~10資安菁英實戰培育課程 第3期臺北場(四日) | |
|---|---|
| 活動時間 | **2024/11/2、3、9、10** |
| 活動地點 | **臺北創新實驗室-會議A廳（臺北市內湖區洲子街12號2樓（近捷運港墘站2號出口））** |
| 活動網站 | **https://nicste2.kktix.cc/events/113elitecourse3** |
| 活動概要 |  <br>**【費用】**<br>免費<br>報名截止： 2024-10-17<br>**【活動內容 / Event Deails】**<br><br>菁英班課程舉辦到今年已經第 4 年了！透過國際級講師傳授資安秘技與實作，獲得一片好評，今年更增添了更多演練與實作內容，讓大家不侷限於紙上談兵，而是將所學技術與理論實際操作應用，可以把課程所學正式內化成自己的能力！ |

不論您是在一般企業、政府單位、資安公司或是其他單位的在職資安技術/研發人員，都歡迎踴躍報名！此次活動將由政府全額補助，所以名額有限，千萬要把握機會喔~

| 《第 3 期臺北場課程資訊》 | |
|---|---|
| 113 年 11 月 2 日至 3 日 (週六、週日) | 藍隊解壓縮 - 從零開始建構企業防禦工事：鄭仲倫講師 |
| 113 年 11 月 9 日(週六) | 雲端保衛戰：藍隊的雲端安全生存指南：林殿智講師 |
| 113 年 11 月 10 日 (週日) | 網路威脅防禦競賽 |

**【主辦單位】國家資通安全研究院**

**【指導單位】數位發展部資通安全署**

**【執行單位】社團法人台灣駭客協會**

**【聯絡窗口】02-2380-0923 鄭規劃師**

mailto:te-atc@nics.nat.gov.tw

## 【TWCERT/CC】APCERT資安年會

| | |
|---|---|
| **活動時間** | **2024/11/5~7** |
| **活動地點** | **台北萬豪酒店(台北市中山區樂群二路199號)** |
| **活動網站** | **https://apcert2024con.org.tw/** |

| | |
|---|---|
| **活動概要** | **【費用】**<br>免費<br>報名截止： 2024-10-30<br><br>**【活動內容 / Event Deails】**<br>亞太區電腦事件協調組織(APCERT)將於2024年11月5日至7日在台北萬豪酒店舉辦年度重要活動—「APCERT 2024會員年會暨國際資安研討會」。此次年會由台灣電腦網路危機處理暨協調中心(TWCERT/CC)主辦，主題為「Power of Together: More Than the Sum of AP CERTs/CSIRTs」。<br>本屆年會將分為兩部分：11月5日至6日為APCERT會員年會及閉門會議，11月7日則與全球最大的資安應變與安全組織Forum for Incident Response and Security Teams共同舉辦公開研討會。該公開研討會將針對多個資安主題進行深入探討，包括資安威脅趨勢、威脅情報與分析、新興技術、治理與管理，以及協作模式等。此次活動旨在促進亞太地區資安專家的交流，並增強各成員間的合作能力，以更有效地應對日益嚴峻的網路安全威脅。APCERT自2003年成立以來，一直致力於建立亞太地區資安專家互信社群，並在面對重大資安事件時提供跨國協作應變的支持。<br>歡迎各界專業人士參加，共同分享最新的資安洞見與技術經驗，攜手提升整體的資安防護能力。<br>**【主辦單位】**亞太區電腦事件協調組織（APCERT）、台灣電腦網路危機處理暨協調中心（TWCERT/CC） |

- **TWCERT/CC 資安活動紀事**

## 113年企業攻防演練成功落幕：TWCERT/CC攜手40家企業強化資安防護

| 量能 | |
|---|---|
| **活動時間** | **113.10.14** |
| **活動概要** | 臺灣電腦網路危機處理暨協調中心(TWCERT/CC)於10月14日舉辦「2024企業藍隊演練」，透過讓企業實際參與資安攻防演練、累積相關實戰經驗，幫助TWCERT/CC企業會員深入了解發生資安事件的原因、事件調查方向與實務做法，提升企業資安事件應變的調查能力，進而提升企業的資通安全防護能量。<br><br>國家資通安全研究院院長何全德致詞時表示，提升資安韌性是當前企業數位轉型的重要課題。臺灣是全球高科技產業的核心，也是許多駭客攻擊的焦點。何院長強調，面對層出不窮之勒索病毒、進階持續性威脅(Advanced Persistent Threat, APT)及新興的AI相關威脅，企業必須加強資安防護，不僅要保障自身及客戶的敏感資訊，還要主動應對各種潛在的網路威脅。此外，企業也應重視資安防護技術的提升及資安人員的專業培訓，才能確保企業具備應對資安事件與快速恢復的能力，以及面對不斷變化及日漸嚴峻的各種資安挑戰。<br><br>TWCERT/CC辦理企業攻防演練已行之有年，去年舉辦的企業藍隊演練獲得企業會員熱烈響應，今年「2024企業藍隊演練」擴大舉辦，共邀請40個TWCERT/CC企業會員組隊參賽。參演團隊需要利用有限資訊，在模擬環境中還原駭客入侵軌跡，並找出入侵根因、阻斷駭客攻擊，以確保其資通系統持續營運不中斷。所有參演團隊在演練期間皆展現了不凡的應變能力與技術水準，經由參與演練的實作經驗，參演的企業紛紛表示更有信心面對今後詭譎多變的資安威脅。<br><br>TWCERT/CC表示，為協助資通安全管理法納管對象以外的民間企業提升資安防護量能，數位發展部責成資安院自113年1月接手運營TWCERT/CC，提供全年24小時不間斷的資安事件通報、情資分 |

享、應變協調、國際合作、意識提升等各項企業資安服務工作。今年11月22日TWCERT將舉辦「2024台灣資安通報應變年會」，邀請對資安公私協作有興趣的各界人士參與，一起與TWCERT企業會員及產官學研各界資安專家，共同分享資安防護經驗與最新的資安趨勢。


| 113年台灣 CERT/CSIRT 聯盟資安教育訓練(台北場) | |
|---|---|
| 活動時間 | 113.10.17 |

**活動概要**

TWCERT/CC於113年10月17日(四)假臺北市「IEAT國際會議中心」舉行113年第2場台灣CERT/CSIRT 聯盟資安教育訓練，本次訓練特別邀請到長庚大學資訊管理學系許晉銘教授，講述「資安事件處理的準備與作業方式」與「資安事件通報與應變指引」，並輔以新興資安議題與趨勢，提供全面且實用的資安知識。

講師簡介：長庚大學資訊管理學系 許晉銘教授

*長庚大學資訊管理系兼任助理教授

*政治大學資安碩士學位學程 兼任助理教授級專業技術人員

*國際鑑識廠商Opentext 認證講師

*國際鑑識廠商Magnet 認證講師

*國際資安廠商EC-Council 認證講師

*金融研訓院 菁英講座

參與者學習如何建立有效的資安事件應變機制，掌握快速準確的通報流程，以及了解最新的資安威脅與防護策略。本課程旨在提升企業的整體資安意識和應變能力，協助建立更安全的數位環境。無論是資安專業人員還是企業決策者，都能從中獲得寶貴的洞見和實務技能。

活動時間：113年10月17日(四) 14:30 – 17:00

活動議程：

| 時間 | 議題 | 講師 |
|---|---|---|
| 14:00 – 14:30 | 報到 | |
| 14:30 – 15:30 | 講題一：資安事件處理的準備與作業方式 | 長庚大學資訊管理學系 許晉銘教授 |
| 15:30 – 15:40 | 休息/茶敘時間 | |
| 15:40 – 16:40 | 講題二：資安事件通報與應變指引 | 長庚大學資訊管理學系 許晉銘教授 |

| | |
|---|---|
| 16:40 – 17:00 | 意見交流 |

# 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：**

| 互動資通Team+企業私有雲溝通協作平台 - SQL Injection | |
|---|---|
| **TVN / CVE ID** | TVN-202410001 / CVE-2024-9921 |
| **CVSS** | 9.8 (Critical)<br>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | Team+ v13.5.x |
| **問題描述** | 互動資通Team+企業私有雲溝通協作平台未妥善驗證特定頁面參數，未經身分鑑別之遠端攻擊者可注入任意SQL指令讀取、修改及刪除資料庫內容。 |
| **解決方法** | 請更新至 v14.0.0(含)以後版本 |
| **公開日期** | 2024-10-14 |
| **相關連結** | **https://www.twcert.org.tw/newepaper/cp-151-8124-d9b92-3.html** |

| 桓基科技 OAKlouds - Arbitrary File Read And Delete | |
|---|---|
| **TVN / CVE ID** | TVN-202410004 / CVE-2024-9924 |
| **CVSS** | 9.8 (Critical)<br>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | 受影響之套件版號：<br>OAKlouds-webbase-2.0 1162(不含)以前版本<br>OAKlouds-webbase-3.0 1162(不含)以前版本 |
| **問題描述** | 桓基科技 OAKlouds 特定套件因 CVE-2024-26261 弱點未完整修補故仍存在風險，未經身分鑑別之遠端攻擊者可下載任意系統檔案，且該檔案下載完後有機會被刪除。 |

| | |
|---|---|
| **解決方法** | 更新 OAKlouds-webbase-2.0 至 1162(含)以後版本<br>更新 OAKlouds-webbase-3.0 至 1162(含)以後版本 |
| **公開日期** | 2024-10-14 |
| **相關連結** | https://www.twcert.org.tw/tw/cp-132-8130-89bb1-1.html |

| 新人類科技資訊 WebEIP v3.0 - SQL injection | |
|---|---|
| **TVN / CVE ID** | TVN-202410005 / CVE-2024-9968 |
| **CVSS** | 8.8 (High)<br>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | WebEIP v3.0 |
| **問題描述** | 新人類科技資訊 WebEIP v3.0 並未妥善驗證使用者輸入，允許已取得一般權限之遠端攻擊者注入SQL指令讀取、修改、刪除資料庫內容。受影響產品已不再進行維護，建議更換至新版產品。 |
| **解決方法** | 廠商表示WebEIP v3.0自釋出已逾15年，目前已停止提供服務與維護，建議更換至WebEIP Pro新版產品 |
| **公開日期** | 2024-10-15 |
| **相關連結** | https://www.twcert.org.tw/tw/cp-132-8132-160bb-1.html |

| 新人類資訊 FlowMaster BPM Plus - Privilege Escalation | |
|---|---|
| **TVN / CVE ID** | TVN-202410007 / CVE-2024-9970 |
| **CVSS** | 8.8 (High)<br>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | FlowMaster BPM Plus Service Pack v5.3.1(不含)以前版本 |

| | |
|---|---|
| **問題描述** | 新人類資訊 FlowMaster BPM Plus存在權限提升漏洞，已取得一般權限的遠端攻擊者可透過竄改特定cookie將權限提升至管理者權限。 |
| **解決方法** | 更新 Service Pack 至 v5.3.1(含)以後版本 |
| **公開日期** | 2024-10-15 |
| **相關連結** | https://www.twcert.org.tw/tw/cp-132-8136-4d5b4-1.html |

| 新人類資訊 FlowMaster BPM Plus - SQL Injection | |
|---|---|
| **TVN / CVE ID** | TVN-202410008 / CVE-2024-9971 |
| **CVSS** | 8.8 (High)<br>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | FlowMaster BPM Plus Service Pack v5.3.1(不含)以前版本 |
| **問題描述** | 新人類資訊 FlowMaster BPM Plus特定查詢功能未妥善限制使用者輸入，允許已獲得一般權限的遠端攻擊者注入SQL指令讀取、修改、刪除資料庫內容。 |
| **解決方法** | 更新 Service Pack 至 v5.3.1(含)以後版本 |
| **公開日期** | 2024-10-15 |
| **相關連結** | https://www.twcert.org.tw/tw/cp-132-8138-d2bb7-1.html |

| 昌佳企業財產管理資訊系統 - SQL Injection | |
|---|---|
| **TVN / CVE ID** | TVN-202409024 / CVE-2024-9972 |
| **CVSS** | 9.8 (Critical)<br>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | 財產管理資訊系統 |

| | |
|---|---|
| **問題描述** | 昌佳企業財產管理資訊系統存在SQL Injection漏洞，允許未經身分鑑別之遠端攻擊者注入任意SQL指令以讀取、修改及刪除資料庫內容。 |
| **解決方法** | 聯繫廠商進行修補 |
| **公開日期** | 2024-10-15 |
| **相關連結** | **https://www.twcert.org.tw/tw/cp-132-8140-ee91e-1.html** |

| **台灣數位學習科技 ee-class - SQL Injection** | |
|---|---|
| **TVN / CVE ID** | TVN-202410010 / CVE-2024-9980 |
| **CVSS** | 8.8 (High)<br>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | ee-class 20240326.13r14494(不含)以前版本 |
| **問題描述** | 台灣數位科技ee-class未妥善驗證特定頁面參數，允許已取得一般權限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 20240326.13r14494(含)以後版本 |
| **公開日期** | 2024-10-15 |
| **相關連結** | **https://www.twcert.org.tw/tw/cp-132-8142-cf0d3-1.html** |

| **台灣數位學習科技 ee-class - Local File Inclusion** | |
|---|---|
| **TVN / CVE ID** | TVN-202410011 / CVE-2024-9981 |
| **CVSS** | 8.8 (High)<br>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | ee-class 20240326.13r14494(不含)以前版本 |

| | |
|---|---|
| **問題描述** | 台灣數位科技ee-class未妥善驗證特定頁面參數，允許已取得一般權限之遠端攻擊者，可先上傳惡意php檔案，再利用此漏洞引用該檔案後於伺服器上執行任意程式碼。 |
| **解決方法** | 更新至 20240326.13r14494(含)以後版本 |
| **公開日期** | 2024-10-15 |
| **相關連結** | https://www.twcert.org.tw/tw/cp-132-8144-2885b-1.html |

| **ESi直通國際 AIM LINE行銷平台 - SQL Injection** | |
|---|---|
| **TVN / CVE ID** | TVN-202410012 / CVE-2024-9982 |
| **CVSS** | 9.8 (Critical)<br>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | AIM LINE行銷平台 3.3 至 5.8.4 版本 |
| **問題描述** | ESi直通國際 AIM LINE行銷平台，在LINE活動模組啟用的情況下未妥善驗證特定查詢參數，未經身分鑑別之遠端攻擊者可注入任意 FetchXml 指令讀取、修改及刪除資料庫內容。 |
| **解決方法** | 聯繫廠商安裝修補程式或升級至6.0(含)以上版本 |
| **公開日期** | 2024-10-15 |
| **相關連結** | https://www.twcert.org.tw/tw/cp-132-8146-497a2-1.html |

| **立即科技企業雲端資料庫 - Missing Authentication** | |
|---|---|
| **TVN / CVE ID** | TVN-202410014 / CVE-2024-9984 |
| **CVSS** | 9.8 (Critical)<br>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |

| | |
|---|---|
| **影響產品** | 企業雲端資料庫 2024/08/08 09:45:25(不含)以前版本 |
| **問題描述** | 立即科技企業雲端資料庫對特定功能之存取未進行身分驗證，未經身分鑑別之遠端攻擊者可存取該功能取得任意使用者的 session cookie. |
| **解決方法** | Update to version 2024/08/08 09:45:25 or later. |
| **公開日期** | 2024-10-15 |
| **相關連結** | https://www.twcert.org.tw/tw/cp-132-8150-c955a-1.html |

| 立即科技企業雲端資料庫 - Arbitrary File Upload | |
|---|---|
| **TVN / CVE ID** | TVN-202410015 / CVE-2024-9985 |
| **CVSS** | 8.8 (High)<br>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | 企業雲端資料庫 2024/08/08 09:45:25(不含)以前版本 |
| **問題描述** | 立即科技企業雲端資料庫未妥善驗證上傳檔案類型，已取得一般權限的攻擊者可上傳網頁後門程式，並利用該後門程式於遠端伺服器執行任意程式碼。 |
| **解決方法** | 更新至 2024/08/08 09:45:25(含)以後版本 |
| **公開日期** | 2024-10-15 |
| **相關連結** | https://www.twcert.org.tw/tw/cp-132-8152-09e81-1.html |

| 中興保全科技 WRTR-304GN-304TW-UPSC - OS Command Injection | |
|---|---|
| **TVN / CVE ID** | TVN-202410016 / CVE-2024-10118 |
| **CVSS** | 9.8 (Critical)<br>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | WRTR-304GN-304TW-UPSC V02 |

| | |
|---|---|
| **問題描述** | 中興保全科技 WRTR-304GN-304TW-UPSC 之特定功能未妥善過濾使用者輸入，未經身分鑑別之遠端攻擊者可利用此漏洞注入任意系統指令並於設備上執行。 |
| **解決方法** | 該產品已不再維護，建議汰換設備 |
| **公開日期** | 2024-10-18 |
| **相關連結** | **https://www.twcert.org.tw/tw/cp-132-8154-69fa5-1.html** |

| **中興保全 WRTM326 - OS Command Injection** | |
|---|---|
| **TVN / CVE ID** | TVN-202410017 / CVE-2024-10119 |
| **CVSS** | 9.8 (Critical)<br>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | WRTM326 2.3.20(不含)以前版本 |
| **問題描述** | 中興保全無線路由器 WRTM326 未妥善驗證特定參數，未經身分鑑別之遠端攻擊者，可藉由發送特製請求執行任意系統指令。 |
| **解決方法** | 更新 WRTM326 至 2.3.20(含)以後版本 |
| **公開日期** | 2024-10-18 |
| **相關連結** | **https://www.twcert.org.tw/tw/cp-132-8156-81c9d-1.html** |

| **葳橋資訊行政管理資訊系統 - Arbitrary File Upload** | |
|---|---|
| **TVN / CVE ID** | TVN-202410019 / CVE-2024-10201 |
| **CVSS** | 8.8 (High)<br>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | 行政管理資訊系統 |
| **問題描述** | 葳橋資訊行政管理資訊系統未妥善驗證上傳檔案類型，已取得一般權限之遠端攻擊者可上傳網頁後門程式並執行。 |

| | |
|---|---|
| **解決方法** | 聯繫廠商進行修補 |
| **公開日期** | 2024-10-21 |
| **相關連結** | **https://www.twcert.org.tw/tw/cp-132-8160-756b6-1.html** |

| **葳橋資訊行政管理資訊系統 - OS Command Injection** | |
|---|---|
| **TVN / CVE ID** | TVN-202410020 / CVE-2024-10202 |
| **CVSS** | 8.8 (High)<br>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| **影響產品** | 行政管理資訊系統 |
| **問題描述** | 葳橋資訊行政管理資訊系統存在OS Command Injection漏洞，允許已取得一般權限之遠端攻擊者注入任意OS指令並執行。 |
| **解決方法** | 聯繫廠商進行修補 |
| **公開日期** | 2024-10-21 |
| **相關連結** | **https://www.twcert.org.tw/tw/cp-132-8162-dc491-1.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10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/**