TWCERT/CC 資安情資電子報

2024 年 4 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)平台之漏洞嚴重程度前五的產品漏洞資訊。

目錄

內容

目錄 II

第 1 章、封面故事 1

建立安全的雲端環境：身分認證與存取管理實務(上) 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 APT組織TODDYCAT正在竊取你的資料 4

2.2 軟體系統資安議題 6

2.2.1 快更新！PALO ALTO NETWORKS CVE-2024-3400已被利用 6

2.3 軟硬體漏洞資訊 8

2.3.1 D-Link NAS存在高風險安全漏洞(CVE-2024-3272與CVE-2024-3273) 8

2.3.2 Palo Alto Networks PAN-OS存在高風險安全漏洞(CVE-2024-3400) 9

2.3.3 Microsoft Windows存在高風險安全漏洞(CVE-2024-21338) 10

2.3.4 XZ Utils存在高風險安全漏洞(CVE-2024-3094) 12

2.3.5 Ivanti EPM Cloud Services Appliance (CSA)存在高風險安全漏洞(CVE-2021-44529) ... 14

2.3.6 Fortinet FortiClientEMS存在高風險安全漏洞(CVE-2023-48788) 15

第 3 章、資安研討會及活動 16

第 4 章、TVN 漏洞公告 25

編輯：TWCERT/CC 團隊 28

第 1 章、封面故事

建立安全的雲端環境：身分認證與存取管理實務(上)

雲端已經不是最新穎的技術，是許多企業經歷數年的雲端旅程，目前雲端服務供應商仍持續透過新的功能和服務不斷演進，然而快速的變動和成長不僅讓企業難以跟上，還有許多企業不慎將安全漏洞引入其環境中。近期CISA釋出「Use Secure Cloud Identity and Access Management Practices」，以嚴格的身份認證和存取控制策略，來確保雲端資料的安全與完整性，本篇我們將先擷取身份管理(Identity Management)內容進行介紹。

- 多因子認證(Multi-factor authentication,MFA)

單一因子認證容易受到憑證竊取、偽造及在多個系統中重複使用的影響，雲端帳戶常常可在全球範圍內存取，因此更容易受到某些類型的單一因子認證弱點的影響。

多因子認證(MFA)能夠提升用戶驗證的安全性，進一步強化防範用戶帳戶被入侵，MFA要求用戶在登入時提供兩個或更多因子：用戶知道的東西、擁有的東西或身份的特徵，通常表示除了密碼外，需要提供第二因子，例如隨機生成的數字代碼、生物特徵(如指紋或臉部識別)或實體認證設備(硬體的唯一識別碼：自然人憑證、通用存取卡等）。

許多類型的MFA都容易受到網路釣魚技術的影響，在可能的情況下，組織應使用抗網路釣魚的MFA方法，例如基於公鑰(PK)的FIDO(Fast Identity Online)/WebAuthn認證方式或基於公鑰基礎設施(PKI)的多因子認證方式(例如CAC/PIV卡)。

- 憑證最佳實務(Credential Best Practices)

錯誤的配置和不當的處理可能會導致使用者憑證受到惡意利用，為了保護憑證的安全，應注意以下幾點：

1. 避免明文儲存：雲端憑證不應以明文形式儲存，若需要，可以利用密碼管理工具管理憑證，例如使用硬體安全模組（HSM）來保護私密金鑰。
2. 停用記住密碼功能：為進一步降低風險，應停用網站或程式的記住密碼功能。
3. 實施多因子身份驗證（MFA）：在可能的情況下，應實施多因子身份驗證，例如使用一次性PIN碼、PKI Token等。

如果無法使用基於PKI的身份驗證，則可以生成私密金鑰，允許應用程序以程式設計方式管理雲端資源。在發行金鑰時，應該妥善處理這些金鑰，因為攻擊者將其視為有價值的目標，CISA也提供一

些建議包括：

1. 最小權限原則：避免使用root或管理權限建立金鑰，並將金鑰僅授予完成操作所需的最低權限
2. 加密儲存：金鑰應由金鑰管理器處理並加密儲存，而不應以明文形式包含在應用程式原始程式碼中或嵌入到二進位檔案中。
3. 使用SSH金鑰：若使用SSH金鑰對連接到雲端託管虛擬機，則應將私鑰儲存在密碼管理器中，並避免共享。

➢ 聯合身份(Identity federation)

在雲端環境中，組織通常會共享身份資訊，以簡化跨環境的身份管理，這種方式稱為聯合身份(Identity federation)，然而，將本地身份與雲端環境的系統聯合在一起，往往成為攻擊者的目標，因為他們希望在不同環境之間輕鬆移動。為了確保整體安全，保護與監控聯合身份伺服器至關重要，建議執行以下安全措施：

1. 使用端點偵測和回應系統識別攻擊的意圖，並定期審核以掌握潛在的危害
2. 使用硬體安全模組（HSM）來保護用於聯合身份的憑證和金鑰
3. 實施網路分段原則，以隔離重要伺服器

本篇我們先介紹CISA釋出「Use Secure Cloud Identity and Access Management Practices」的身份管理部分內容，身份管理不論在雲端或是地端伺服器管理都十分重要，身份管理部分亦可檢視地端管理機制是否符合安全需求，以確保組織網路資訊安全。

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

第 2 章、國內外重要資安事件

2.1 新興應用資安

2.1.1 APT組織ToddyCat正在竊取你的資料

ToddyCat 是一個主要針對位於亞太地區的政府機關與國防有關的 APT 組織。該組織的主要目標之一是竊取主機中的敏感資訊，近期卡巴斯基團隊發現ToddyCat已透過一系列複雜的手法取得了工業相關資料。

據2020年的報導，該組織以Exchange Server為攻擊目標，在入侵成功主機上植入木馬程式Ninja Trojan及後門程式Samurai，以便能持續控制設備，並在組織內部進行橫向的擴散。

攻擊活動中，為了從許多主機收集大量資料，攻擊者需儘可能自動化，並使用不同的方式持續掌握並監控被入侵成功的系統。卡

巴期基研究團隊表示在這次的攻擊活動中，ToddyCat入侵成功後，使用了多種工具來建立多個對外通道，即使其中一個通道被發現並清除，他們仍然可以存取系統，以確保能持續控制遠端主機，包含反向SSH通道、SoftEther VPN、Ngrok、Kron、FRP client等工具，

卡巴期基研究團隊亦發現ToddyCat使用新的資料蒐集工具，並取名為cuthead，可以用來搜尋特定副檔名或特定的名稱，同時ToddyCat亦利用TomBerBil工具蒐集瀏覽器所儲存的cookie與密碼，進一步竊取敏感資料。

另外，ToddyCat針對通訊軟體WhatsApp資訊也會進行蒐集，依據目前分析情況，其所搜集的內容為網頁版的資料，主因是瀏覽器會將資料儲存在用戶端主機，內容包含了詳細的個人資料、聊天資料、聊天對象的電話號碼及 session 資料，並可以透過名為WAExp的工具複製儲存內容，WAExp會先確認使用者所在的目錄，依Chrome、Edge和Mozilla不同瀏覽器的目錄取得相關檔案，再將取得的資料儲存在特定目錄以取得這些資料。

研究人員發現ToddyCat利用各種工具持續連線到目標主機，且透過自動化的方式搜尋並蒐集有興趣的資料，同時也以不同方式繞過各種防護技術，避免連線程式被系統所偵測。

為了保護組織設備的安全，研究人員建議將提供流量通道的雲端服務資源及IP位址加到防火牆的阻擋清單中，另限制管理者可使用的遠端連線工具，且禁止或監控未經允許的程式。此外，應該要求使用者避免在瀏覽器中儲存密碼，這可讓攻擊者容易取得敏感的資料。

- 資料來源：
  1. ToddyCat is making holes in your infrastructure
  2. ToddyCat: Keep calm and check logs
  3. Unveiling an unknown APT actor attacking high-profile entities in Europe and Asia

2.2 軟體系統資安議題

2.2.1 快更新！Palo Alto Networks CVE-2024-3400已被利用

Palo Ato Networks發出告警，該公司PAN-OS防火牆存在命令注入漏洞(Command Injection)，使未經身份驗證的攻擊者能夠在防火牆以root權限執行任意程式碼，並已經在被大量利用攻擊中，建議使用者儘速採取緩解措施或進行更新作業。

Palo Ato Networks表示漏洞存在於設置GlobalProtect gateway或GlobalProtect portal(或兩者)功能的PAN-OS 10.2、PAN-OS 11.0和PAN-OS 11.1防火牆，受影響版本如下：

PAN-OS < 10.2.9-h1
PAN-OS <11.0.4-h1
PAN-OS < 11.1.2-h3

Palo Ato Networks安全研究組織Unit42發現此漏洞概念性驗證(Proof of Concept，PoC)攻擊程式已經由第三方公開於網路，利用此漏洞的攻擊數量不斷增加。在資安威脅情報研究公司Volexity擴大調查後，發現自2024年3月26日起，多個公司和組織遭受攻擊者利用這

個漏洞的攻擊，而且，攻擊者疑似透過在火牆設備上放置Zore-bytes文件以驗證漏洞可利用性。另外，在4月7日Volexity觀察到攻擊者嘗試在使用者端的防火牆部署後門程式，但未成功。4月10日，即發現攻擊者成功地植入了惡意Payload，並下載其它惡意程式，以便進行內部橫向移動和竊取憑證和檔案。

Palo Ato Networks提供用戶透過PAN-OS CLI 的命令，協助辨識裝置上是否有此漏洞被攻擊的跡象：

1.搜尋 gpsvc.log相關紀錄檔

- **grep pattern "failed to unmarshal session(.\+.\/" mp-log gpsvc.log***

2.若搜尋到的記錄中，”session(“ 與 ”)” 之間的值不像是GUID，而是檔案的路徑或嵌入式shell命令，即需要進一步確認是否與CVE-2024-3400相關。

可能遭利用之輸出結果如下：

- **failed to unmarshal session(../../some/path)**

正常輸出結果如下：

- **failed to unmarshal session(01234567-89ab-cdef-1234-567890abcdef)**

Palo Ato Networks已針對CVE-2024-3400釋出更新程式，使用者除了透過官方提供檢測方式自行檢測外，亦應儘速完成更新作業，避免遭有心人士利用漏洞入侵。

- 資料來源：

1. CVE-2024-3400 PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalP
2. Threat Brief: Operation MidnightEclipse, Post-Exploitation Activity Related to CVE-2024-3400

2.3 軟硬體漏洞資訊

2.3.1 D-Link NAS存在高風險安全漏洞(CVE-2024-3272與CVE-2024-3273)

CVE 編號	CVE-2024-3272 與 CVE-2024-3273
影響產品	D-Link
解決辦法	官方已宣布不再支援更新受影響之型號，請儘速確認並進行汰換。

- 內容說明：

  研究人員發現部分舊款 D-Link NAS 存在使用 Hard-coded 帳號通行碼漏洞(Use of Hard-Coded Credentials)(CVE-2024-3272)與作業系統指令注入漏洞(OS Command Injection)(CVE-2024-3273)，未經身分鑑別之遠端攻擊者可利用 CVE-2024-3272 提升至系統權限，或利用 CVE-2024-3273 執行任意程式碼。受影響之型號皆已停止支援，請儘速確認並進行汰換。

- 影響平台：

  受影響型號如下：

  DNS-320L
  DNS-325
  DNS-327L
  DNS-340L

- 資料來源：

  1. https://nvd.nist.gov/vuln/detail/CVE-2024-3272
  2. https://nvd.nist.gov/vuln/detail/CVE-2024-3273
  3. https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383

2.3.2 Palo Alto Networks PAN-OS存在高風險安全漏洞(CVE-2024-3400)

CVE 編號	CVE-2024-3400
影響產品	PAN-OS
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： PAN-OS 10.2 系列請更新至 10.2.9-h1(含)以後版本 PAN-OS 11.0 系列請更新至 11.0.4-h1(含)以後版本 PAN-OS 11.1 系列請更新至 11.1.2-h3(含)以後版本

- 內容說明：

  研究人員發現 Palo Alto Networks PAN-OS 存在作業系統命令注入(OS Command Injection)漏洞(CVE-2024-3400)，未經身分鑑別之遠端攻擊者，可利用此漏洞於防火牆以最高權限(root)執行任意程式碼。該漏洞目前已遭駭客利用，請儘速確認並進行修補。

- 影響平台：

  受影響版本如下：

  PAN-OS 10.2.9-h1(不含)以前版本

  PAN-OS 11.0.4-h1(不含)以前版本

  PAN-OS 11.1.2-h3(不含)以前版本

- 資料來源：

  1. https://nvd.nist.gov/vuln/detail/CVE-2024-3400
  2. https://security.paloaltonetworks.com/CVE-2024-3400
  3. https://www.ithome.com.tw/news/162282

2.3.3 Microsoft Windows存在高風險安全漏洞(CVE-2024-21338)

CVE 編號	CVE-2024-3400
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/vulnerability/CVE-2024-21338

- 內容說明：

  研究人員發現 Microsoft Windows 作業系統的 AppLocker 安全功能存在本機提權漏洞(CVE-2024-21338)，允許完成身分鑑別的本機端攻擊者，利用此漏洞提升至系統權限。該漏洞目前已遭駭客利用，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://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://nvd.nist.gov/vuln/detail/CVE-2024-21338
3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21338

2.3.4 XZ Utils存在高風險安全漏洞(CVE-2024-3094)

CVE 編號	CVE-2024-3094
影響產品	XZ Utils 5.6.0 與 5.6.1
解決辦法	請考處置建議

- 內容說明：

  研究人員發現 XZ Utils 資料壓縮程式庫已遭受供應鏈攻擊(Supply Chain Attack)(CVE-2024-3094)，該程式之特定版本已被植入後門程式，並有部分 Linux 發行版本安裝受影響之 XZ Utils 版本，請儘速確認並依官方建議採取對應措施。

- 影響平台：

  受影響之 Linux 作業系統如下：

  - Alpine
  - Debian (testing、unstable 及 experimental)
  - Fedora 41、Fedora Rawhide 及 Fedora Linux 40 beta
  - Kali Linux
  - openSUSE Tumbleweed 與 openSUSE MicroOS

- 處置建議：

  確認版本後，請配合官方說明確認是否需要更新或是降低 XZ Utils 版本

  - Alpine：
    https://security.alpinelinux.org/vuln/CVE-2024-3094
  - Debian：

https://security-tracker.debian.org/tracker/CVE-2024-3094

- Fedora：
  https://fedoramagazine.org/cve-2024-3094-security-alert-f40-rawhide/
- Kali Linux：
  https://www.kali.org/blog/about-the-xz-backdoor/
- openSUSE：
  https://www.suse.com/security/cve/CVE-2024-3094.html
  https://news.opensuse.org/2024/03/29/xz-backdoor/

- 於 Linux 作業系統透過以下指令確認 XZ Utils 的版本，以了解是否受本弱點影響：

  $ xz –version
  $ strings `which xz` | grep '5\.6\.[01]'

- 若是使用 Alpine 作業系統，請使用以下指令確認：

  $ apk list xz

- 資料來源：

1. https://nvd.nist.gov/vuln/detail/CVE-2024-3094
2. https://jfrog.com/blog/xz-backdoor-attack-cve-2024-3094-all-you-need-to-know
3. https://unit42.paloaltonetworks.com/threat-brief-xz-utils-cve-2024-3094/
4. https://www.ithome.com.tw/news/162040
5. https://security.alpinelinux.org/vuln/CVE-2024-3094
6. https://security-tracker.debian.org/tracker/CVE-2024-3094
7. https://fedoramagazine.org/cve-2024-3094-security-alert-f40-rawhide/
8. https://www.kali.org/blog/about-the-xz-backdoor/
9. https://www.suse.com/security/cve/CVE-2024-3094.html
10. https://news.opensuse.org/2024/03/29/xz-backdoor/

2.3.5 Ivanti EPM Cloud Services Appliance (CSA)存在高風險安全漏洞(CVE-2021-44529)

CVE 編號	CVE-2021-44529
影響產品	Ivanti EPM Cloud Services Appliance (CSA)
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： CSA 4.6.0-512(含)以後版本

- 內容說明：

  研究人員發現 Ivanti EPM Cloud Services Appliance (CSA)存在程式碼注入(Code Injection)漏洞(CVE-2021-44529)，未經身分鑑別之遠端攻擊者可利用此漏洞，於系統上以受限的權限(nobody)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：

  CSA 4.6.0-512(不含)以前版本

- 資料來源：

  1. https://forums.ivanti.com/s/article/SA-2021-12-02?language=en_US
  2. https://nvd.nist.gov/vuln/detail/CVE-2021-44529

2.3.6 Fortinet FortiClientEMS存在高風險安全漏洞(CVE-2023-48788)

CVE 編號	CVE-2023-48788
影響產品	FortiClientEMS
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： FortiClientEMS 7.2.3(含)以後版本 FortiClientEMS 7.0.11(含)以後版本

- 內容說明：

  研究人員發現 Fortinet FortiClientEMS 存在資料庫注入(SQL Injection)漏洞(CVE-2023-48788)，未經身分鑑別之遠端攻擊者，可利用此漏洞新增、刪除或修改資料庫內容。該漏洞已遭駭客利用，請儘速確認並進行修補。

- 影響平台：

  FortiClientEMS 7.2.0 至 7.2.2 版本

  FortiClientEMS 7.0.1 至 7.0.10 版本

- 資料來源：

  1. https://www.fortiguard.com/psirt/FG-IR-24-007
  2. https://nvd.nist.gov/vuln/detail/CVE-2023-48788

第 3 章、資安研討會及活動

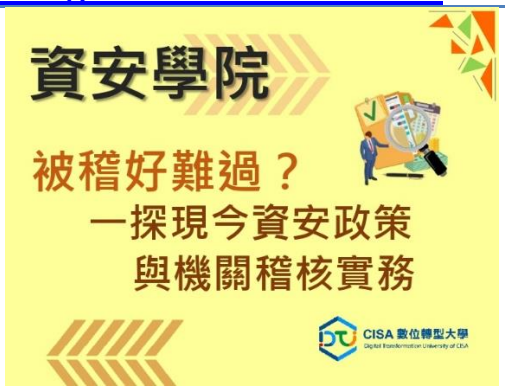
【限定資訊服務業者參與】2024-03-26 ~ 2024-09-30 個人資料檔案安全維護計畫一對一線上健檢諮詢	
活動時間	2024-03-26 ~ 2024-09-30
活動地點	線上活動
活動網站	https://www.cisanet.org.tw/Course/Detail/5286
活動概要	 **活動內容 / Event Deails：** 數產署於 2024 年 10 月 12 日訂定「數位經濟相關產業個人資料檔案安全維護管理辦法」，業者若未採取適當安全維護措施致個資被竊取、竄改、毀損、滅失或洩漏，或未訂定安全維護計畫，可處 2 萬元以上 200 萬元以下罰鍰！ 為協助資訊服務業者遵循《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**

【資策會】5/8 第三方委外與供應鏈資安管理	
活動時間	2024年05月08日(三) 下午 13:00~16:30
活動地點	資安暨智慧科技研發大樓A122第一會議室(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=2421
活動概要	 **活動內容 / Event Deails：** 近年來國際間重大資安事故頻傳，影響範圍擴及生產線、接獲勒索。當遭受網路攻擊時，應如何正確因應、處理及保全數位證據，儼然成為各組織必須正視的課題。本課程將說明當發生資安事故之際，應如何迅速釐清受害範圍、清除惡意程式及阻斷可疑之中繼站連線，進而回復正常運作。並透過模擬環境實作，解析駭客入侵情境，教導您資安事件處理流程及調查入侵事件等一系列因應措施。 **【課程講師】**：遠傳電信朱建國資安長 **【課程對象】**：資訊人員、網路管理人員、資安推動/應用人員 因名額有限本課程採審核制，錄取通知將於開課前一周以 email 發送給錄取者。 **【課程目標】**： 企業第三方委外與供應鏈相關法規簡介

	說明企業第三方委外與供應鏈常見的管理框架，以及可能的資安風險 由供應鏈資安角度來看企業因應之道

【資安學院】5/9-5/10資安事故處理實務演練（實作課）	
活動時間	**2024-05-09 09:00 ~ 2024-05-10 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/5220**
活動概要	 原價：NT 11,500 元/人 軟協會員價：NT 9,200 元/人 費用含稅、教材及完課證明 **活動內容 / Event Deails：** 近年來國際間重大資安事故頻傳，影響範圍擴及生產線、接獲勒索。當遭受網路攻擊時，應如何正確因應、處理及保全數位證據，儼然成為各組織必須正視的課題。本課程將說明當發生資安事故之際，應如何迅速釐清受害範圍、清除惡意程式及阻斷可疑之中繼站連線，進而回復正常運作。並透過模擬環境實作，解析駭客入侵情境，教導您資安事件處理流程及調查入侵事件等一系列因應措施。 **提醒：** 請自備筆記型電腦，至少 8GB 以上記憶體，50G 閒置硬碟空間 **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：**2024-05-02

【資安學院】5/14弱點修補技巧(VMS弱點管理系統)	
活動時間	**2024-05-14 13:30 ~ 2024-05-14 17:30**
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/5233**
活動概要	 原價：NT 4,400 元/人 早鳥價：NT 4,000 元/人(課前一個月報名) 軟協會員價：NT 3,800 元/人 費用含稅、教材及完課證明 **活動內容 / Event Deails：** 為保障資訊資產安全，定期執行弱點掃描或滲透測試是必要的檢測工作。其中，弱點掃描主要用以找出已知、已公開的作業系統、應用程式或設備韌體上的漏洞。然而，在產出弱點掃描報告後，面對一長串的資料又該如何下手？ 本課程將教導學員弱點修補邏輯判斷原則、常見弱點類型、針對各類弱點劃分風險等級並提出改善建議。讓您得以優先處理衝擊最大之弱點、有效地控制風險，進而強化企業資安韌性。 **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：**2024-05-07

【資安學院】5/24被稽好難過？一探現今資安政策與機關稽核實務	
活動時間	**2024-05-24 09:00 ~ 2024-05-24 16:00**
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/5225**
活動概要	 原價：NT 6,900 元/人 早鳥價：NT 6,200 元/人(課前一個月報名) 軟協會員價：NT 5,600 元/人 費用含稅、教材、餐點及完課證明 **活動內容 / Event Deails：** 資通安全管理法自 108 年施行，資通安全稽核已成為納管對象所應辦理的重要法遵事項之一，資通安全管理法也在 112 年起開始進行修法作業。 本次課程將介紹資通安全管理法之重點內容，包括母法及其 6 項子法、維護計畫、防護基準等；同時說明資通安全管理法主管機關所辦理資通安全實地稽核的方式、重點及常見問題。 **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：**2024-05-17

【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	 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 **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	 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 **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。 **備註：** 本課程與 BSI 台灣分公司合作 講師：BSI 台灣分公司專業合格之講師授課 教材：英、中對照教材及試卷。

	證書：BSI 原廠授證。課程測驗通過後，將由 BSI 台灣分公司授予證書；測驗未通過者，本會則將發「結業證書」乙只。 注意事項：本課程需全程參與，不可請假或缺席，請假或缺席時數者不予考試及發證，敬請保留完整上課時間。 **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 本月份發布之嚴重程度前五資安漏洞資訊如下表：

鎧睿全球科技 ArmorX Android APP - MFA Bypass	
TVN / CVE ID	TVN-202404014 / CVE-2024-4303
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	ArmorX Android APP v.1.5.2(含)以前版本
問題描述	鎧睿全球科技ArmorX Android APP登入功能之多因子驗證並未實作完善，遠端攻擊者若已取得使用者帳號密碼，可利用此漏洞規避多因子驗證，並成功登入APP。
解決方法	更新至v.1.5.3(含)以後版本(20230919 釋出)
公開日期	2024-04-29
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-7781-ef309-3.html**

新夥伴科技 N-Reporter 與 N-Cloud - Os Command Injection	
TVN / CVE ID	TVN-202404012 / CVE-2024-4301
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	N-Reporter , N-Cloud Firmware 6.1.187 (20240216-1603)(不含)之前版本
問題描述	新夥伴科技 N-Reporter與N-Cloud 存在 OS Command Injection 漏洞，允許取得一般權限之遠端攻擊者，藉由操縱特定頁面使用者輸入，執行任意系統指令。

解決方法	更新 Firmware 至 6.1.187 (20240216-1603)(含)之後版本
公開日期	2024-04-29
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7776-035ff-3.html

醫位資訊 FS-EZViewer(Web) - Sensitive Data Exposure	
TVN / CVE ID	TVN-202404011 / CVE-2024-4300
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	FS-EZViewer(Web) 10.4.0.X(含)以前版本
問題描述	醫位資訊 FS-EZViewer(Web) 將敏感資訊暴露於服務中，使用者可在未登入的情況下，透過網頁原始碼取得資料庫設定檔路徑，存取該路徑可取得資料庫最高權限之帳號密碼與資料庫主機IP位址，透過此資訊可連線至資料庫，進而新增、修改或刪除資料庫內容。
解決方法	更新至 10.4.1.0(含)以後版本
公開日期	2024-04-29
相關連結	https://www.twcert.org.tw/newepaper/cp-151-7774-fbd01-3.html

ASUS 無線路由器 - OS Command Injection	
TVN / CVE ID	TVN-202404006 / CVE-2024-1655
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	ExpertWiFi EBM63 韌體 3.0.0.6.102_32645(不含)以前版本 ExpertWiFi EBM68 韌體 3.0.0.6.102_44384(不含)以前版本 RT-AX57 Go 韌體 3.0.0.6.102_22188(不含)以前版本

問題描述	ASUS 部分無線路由器型號存在 OS Command Injection 漏洞，允許通過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 ExpertWiFi EBM63 韌體至 3.0.0.6.102_32645(含)以後版本 更新 ExpertWiFi EBM68 韌體至 3.0.0.6.102_44384(含)以後版本 更新 RT-AX57 Go 韌體至 3.0.0.6.102_22188(含)以後版本
公開日期	2024-04-15
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-7737-1acd0-3.html**

人工智能 QbiBot 智能機器人 - Broken Access Control	
TVN / CVE ID	TVN-202404004 / CVE-2024-3777
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	QbiBot 智能機器人 v8.0.4(含)以前版本
問題描述	人工智能 QbiBot 智能機器人忘記密碼功能缺乏適當的存取控制，未經身分鑑別之遠端攻擊者可重設任意使用者密碼。
解決方法	更新至 v8.0.5(含)以上版本或詢問廠商相關修補建議
公開日期	2024-04-15
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-7371-aecf1-3.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 4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**