TWCERT/CC 資安情資電子報

2025 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、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

社交工程手法再升級：結合雲端服務與短期憑證規避防禦

TWCERT/CC 接獲外部情資，近期出現一波結合雲端服務與仿冒網域的社交工程攻擊活動。駭客透過租用 Microsoft 365 服務、註冊近似官方的域名，並申請短期 SSL 憑證，試圖規避郵件與網頁防禦機制，發起釣魚郵件攻擊。

依據情資內容顯示，駭客在第一波攻擊行動中，透過租用的 Microsoft 365 合法電子郵件帳號，偽冒「Microsoft帳戶異常登入活動通知」，針對企業內部多個目標發動釣魚郵件攻擊，要求目標登入帳戶，檢視異常登入通知。此外，攻擊者利用 URL Pattern 篩選目標，若符合規則便顯示客製化釣魚頁面以竊取帳號密碼；不符合則轉向官方合法登入頁面。

圖1：針對多個目標發送偽冒Microsoft系統通知意圖竊取帳密。資料來源：TWCERT/CC整理

URL Pattern 是一種用來判斷網址是否符合特定格式的規則(如圖2)，「/*」代表所有在 login.example.com 下的頁面。攻擊者可利用這樣的 URL Pattern 精準篩選目標，決定何時顯示釣魚頁面。

圖2：URL Pattern 示意圖，資料來源：TWCERT/CC整理

第二波攻擊行動中，駭客採魚叉式釣魚手法，同樣利用 Microsoft 365 服務，但改為針對特定目標「連續」發送多封偽冒「Microsoft一次

性代碼通知」，企圖營造目標帳戶正遭多次嘗試登入假象，爾後再次寄送偽冒「Microsoft帳戶異常登入活動通知」，引誘目標點選連結立即登入帳戶以檢視異常登入紀錄，進而竊取目標帳號密碼，如圖3所示。

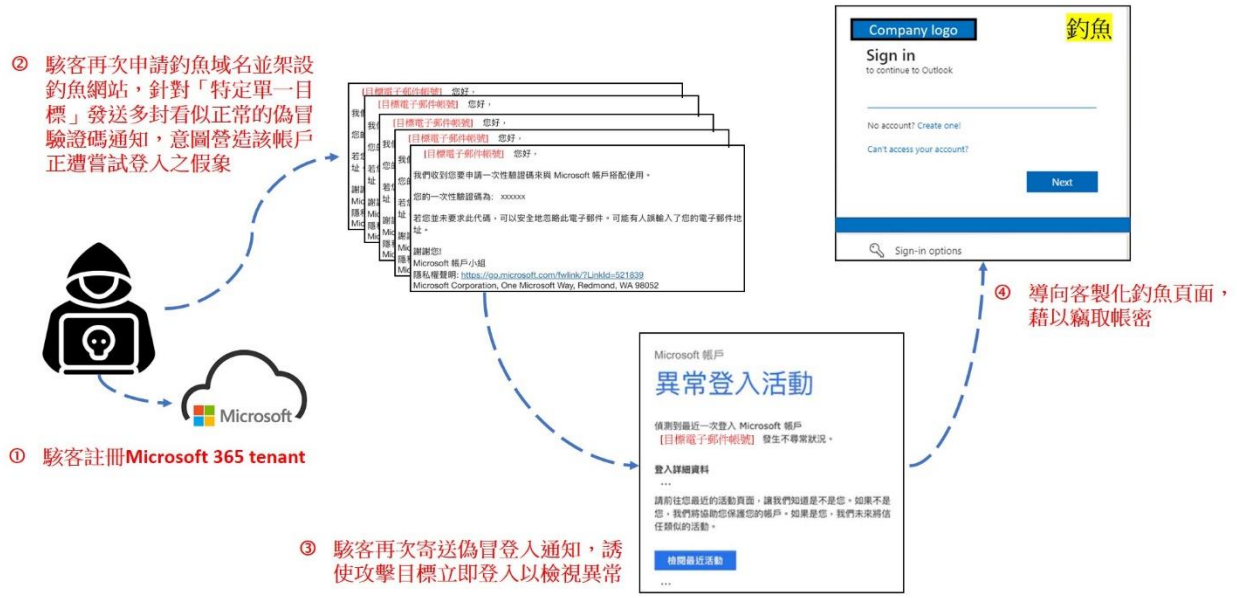


圖3 :針對單一目標多次發送偽冒通知營造急迫氛圍，誘使受害目標輸入帳密。資料來源：TWCERT/CC整理

駭客組織持續升級社交工程與釣魚攻擊手法，此次攻擊採取進階化策略，反覆寄送偽冒的 Microsoft 系統通知，企圖製造緊迫氛圍，利用收件人對官方通知的信任與時間壓力，誘使收件人在未充分確認下點擊惡意連結提供帳號密碼，造成帳戶被未授權存取與敏感資料外洩。TWCERT/CC 提醒企業與民眾保持高度警覺，特別是在收到疑似來自官方電子郵件時，應格外謹慎，以避免成為攻擊目標。

防護措施建議：

1. 建議留意可疑電子郵件，注意郵件來源正確性，不點擊不明的網址或連結，進入可疑網站不輸入個資、帳號密碼及金融資訊。
2. 建議定期更換符合複雜性需求之密碼，並啟用多因子認證(MFA)，以提高安全防護措施。
3. 網路管理人員應參考最新受駭偵測指標，確實實施預防性阻擋措施，以攔截並過濾可疑郵件。
4. 加強內部宣導，提升人員資安意識，以防範駭客利用電子郵件進行社交工程攻擊。

第 2 章、國內外重要資安事件

2.1 資安趨勢

2.1.1 LockBit 5.0 勒索軟體再度活躍，展現更高技術複雜度與跨平台攻擊能力

近期LockBit 5.0 勒索軟體再度現身，並帶來多項技術升級，顯示該勒索家族仍在勒索軟體生態系中維持高度活躍與影響力。LockBit 5.0 不僅強化程式混淆與反向分析防禦機制，更進一步加強其跨平台運作能力。根據趨勢科技研究團隊的樣本分析，LockBit 5.0 已出現可針對 Windows、Linux 與 VMware ESXi 等多種系統環境運作的變種，讓攻擊者能以單一攻擊行為影響混合雲或虛擬化環境，對企業營運造成更大範圍的影響。

根據樣本分析，Window平台的二進位檔案採用大量混淆與打包技術，利用多項反分析技術，包含繞過Event Tracing for Windows(ETW)與終止安全相關服務等方式下，透過DLL反射載入惡意酬載(payload)。

Linux版本則延續類似攻擊手法，並新增針對特定目錄和檔案類型的命令列選項，以提高攻擊精準度。另一個針對VMware虛擬化環境的ESXi變體，能在單次攻擊中加密整個虛擬機器下的基礎架構，進一步擴大營運中斷風險。

檢視LockBit 5.0 windows平台版本，透過-h參數可查詢使用指令，其展現簡潔使用者介面，清楚描述勒索軟體選項與設定，使攻擊者使用能更靈活，如圖1所示。加密檔案的副檔名則以隨機16字元格式呈現，增加復原的難度，如圖2所示。該版本仍保留與受害者互動功能，內建簡易聊天介面方便贖金協商；同時採用地緣政治迴避機制，偵測到俄語系統或俄國地理位置即停止執行。而Linux 版延續Windows 版的核心功能，展現跨平台能力，提供與windows版本相同的操作便利與彈性，這些設計不僅提升攻擊效率，也增加企業資訊安全防護挑戰。另外，VMware ESXi版則是針對虛擬化基礎架構環境上的重大升級，因ESXi主機通常同時承載多台虛擬機，攻擊者可透過單一惡意酬載在主機層級執行加密，迅速波及整個虛擬化環境並造成大規模營運中斷。

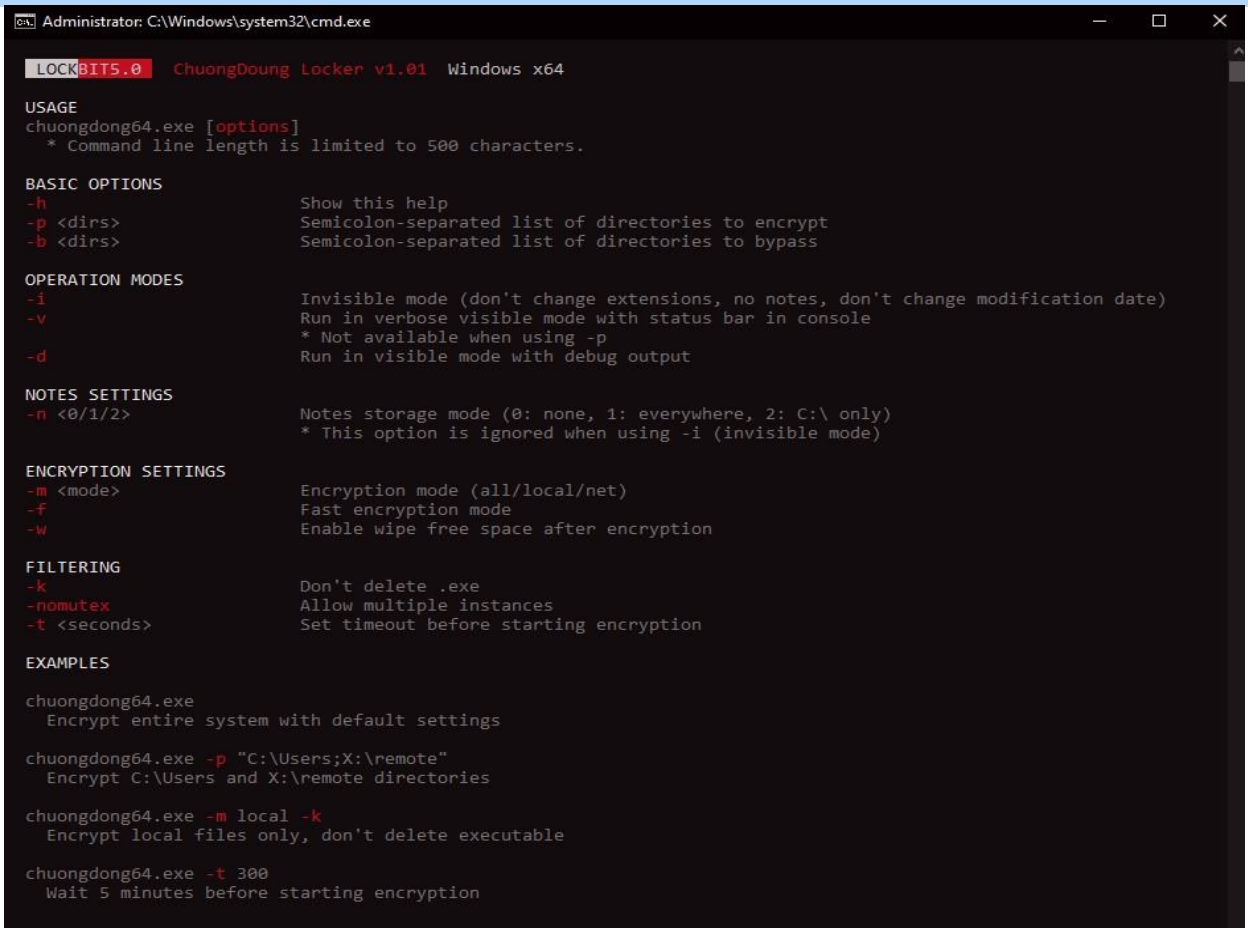


圖1：LockBit 5.0 Windows版的使用者介面。圖片來源：趨勢科技

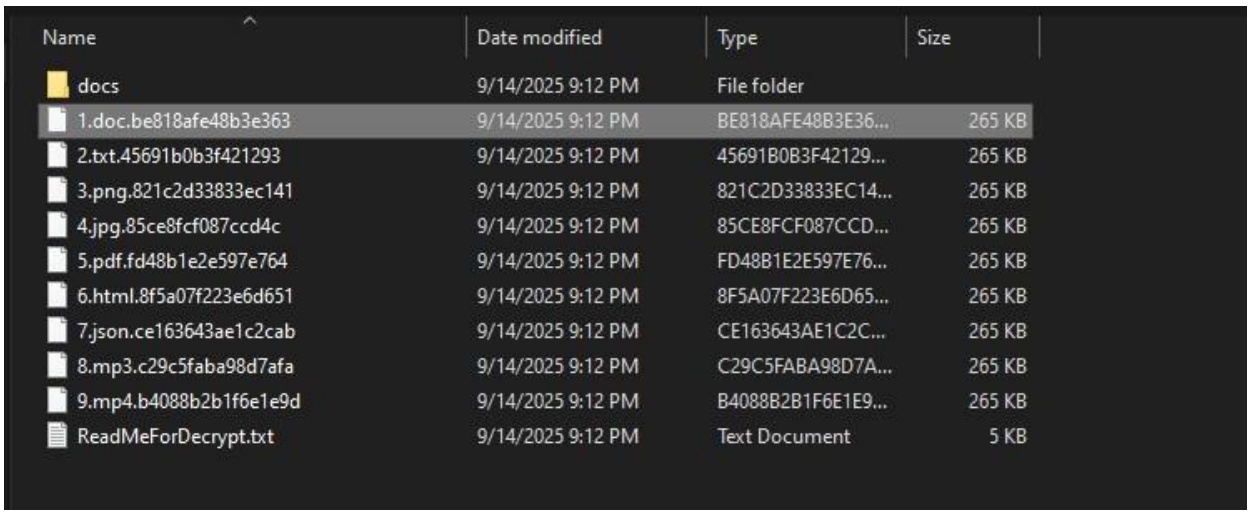


圖2：LockBit 5.0 加密檔案附加隨機生成的副檔名。圖片來源：趨勢科技

面對LockBit 5.0的高技術威脅，企業與組織應積極加強跨平台的資安防護策略，尤其是虛擬化基礎架構的安全監控與管理，TWCERT/CC建議企業應採取以下安全措施：

1. 定期更新並修補所有作業系統和應用軟體
2. 加強勒索軟體偵測與阻擋技術，如部署行為分析與異常監控工具
3. 強化資安意識訓練，警覺勒索軟體的社交工程攻擊
4. 設立嚴格的存取控制與隔離政策，減少橫向移動的風險
5. 定期備份重要資料，並規劃事故後的資料恢復機制

- 相關連結
  1. New LockBit 5.0 Targets Windows, Linux, ESXi
  2. LockBit Ransomware Group Unveils Version 5.0 on Its Sixth Anniversary

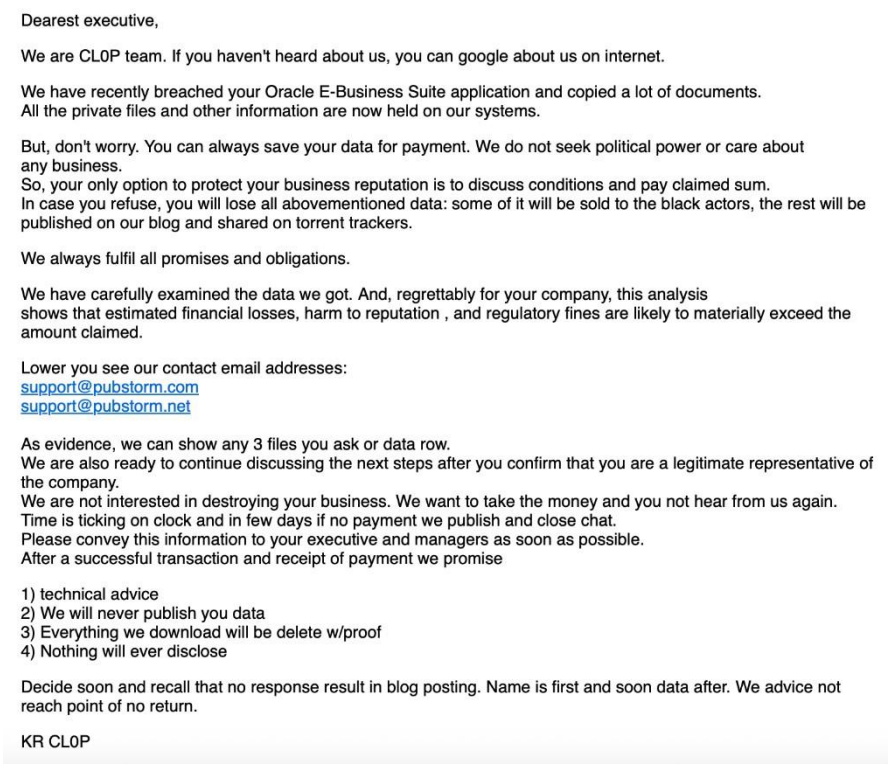
2.2 軟硬體系統資安議題

2.2.1 Oracle E-Business Suite曝嚴重漏洞CVE-2025-61882，恐遭駭客利用入侵

Oracle於2025年10月發布重大資安公告，揭露旗下E-Business Suite 12.2.3至12.2.14版本存在一個高嚴重性漏洞(CVE-2025-61882，CVSS：9.8)。該漏洞允許未經身分驗證的攻擊者透過HTTP協定進行遠端存取，可能導致遠端程式碼執行。美國網路安全與基礎設施安全局（CISA）已將此漏洞納入已知漏洞目錄(KEV)，並觀察該漏洞已被勒索軟體集團積極利用，建議用戶儘速依照Oracle官方建議，採取相關緩解措施，以防止系統遭入侵並造成重大損失。

Google威脅情報小組 (GTIG) 和 Mandiant研究團隊追蹤到與勒索軟體集團「CL0P」相關的攻擊行動，調查報告指出，攻擊者已向多家組織的高階主管發送電子郵件，聲稱已竊取Oracle E-Business Suite環境中的敏感

資料，並藉此施壓受害企業。值得注意的是，這些勒索信件中包含兩個被列入CL0P洩露網站的電子郵件地址，分別為support[@]pubstorm.com和support[@]pubstorm.net，如圖1所示。



Dearest executive,

We are CL0P team. If you haven't heard about us, you can google about us on internet.

We have recently breached your Oracle E-Business Suite application and copied a lot of documents.
All the private files and other information are now held on our systems.

But, don't worry. You can always save your data for payment. We do not seek political power or care about any business.
So, your only option to protect your business reputation is to discuss conditions and pay claimed sum.
In case you refuse, you will lose all abovementioned data: some of it will be sold to the black actors, the rest will be published on our blog and shared on torrent trackers.

We always fulfil all promises and obligations.

We have carefully examined the data we got. And, regrettably for your company, this analysis shows that estimated financial losses, harm to reputation , and regulatory fines are likely to materially exceed the amount claimed.

Lower you see our contact email addresses:
support@pubstorm.com
support@pubstorm.net

As evidence, we can show any 3 files you ask or data row.
We are also ready to continue discussing the next steps after you confirm that you are a legitimate representative of the company.
We are not interested in destroying your business. We want to take the money and you not hear from us again.
Time is ticking on clock and in few days if no payment we publish and close chat.
Please convey this information to your executive and managers as soon as possible.
After a successful transaction and receipt of payment we promise

1) technical advice
2) We will never publish you data
3) Everything we download will be delete w/proof
4) Nothing will ever disclose

Decide soon and recall that no response result in blog posting. Name is first and soon data after. We advice not reach point of no return.

KR CL0P

圖1：CL0P勒索組織發送給受害者的勒索郵件。圖片來源：GTIG

根據watchTowr Labs深入分析，攻擊者利用該漏洞多種複合攻擊技術，包含伺服器端請求偽造(SSRF)、CRLF注入、身分驗證繞過和XSLT注入，形成一條精密而高效的攻擊鏈，攻擊流程及技術如圖2所示。

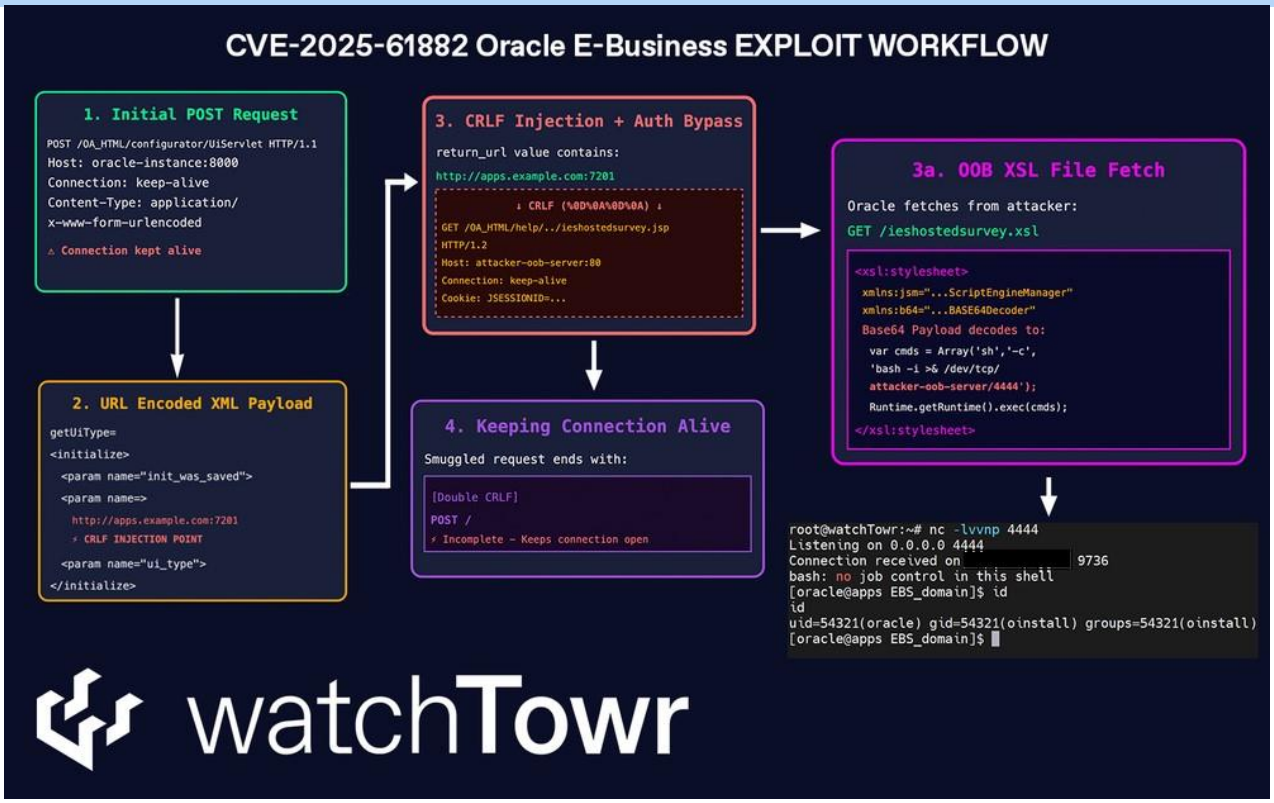


圖2：CVE-2025-61882漏洞利用攻擊鏈。圖片來源：watchTowr Labs

以下為攻擊流程主要階段說明：

第一階段，偽造伺服器端請求 (SSRF)：攻擊者注入特製的XML請求至 Oracle EBS，誘使伺服器向攻擊者指定的 URL 發起 HTTP 請求，藉此取得原本僅能於內部網路存取的資源或資料。

第二階段，注入CRLF：透過注入CRLF字元操控HTTP標頭，將原本的GET請求改寫為POST請求，成功繞過應用系統的安全檢查。

第三階段，持續連線：利用HTTP持續連線機制(keep-alive或connection reuse)，在同一TCP連線中連續發送多個請求，有效提升攻擊成功率且減少被偵測風險。

第四階段，身分驗證繞過：由於Oracle EBS服務綁定至私有IP介面，攻擊者藉由路徑遍歷技巧繞過身份驗證，訪問應受保護的內部管理

頁面，取得更高權限操作能力。

第五階段，XSLT注入：攻擊者控制伺服器下載並注入惡意XSLT，借助Oracle EBS的XSLT處理功能執行惡意Java代碼，以利遠端程式碼執行（RCE），進一步掌控系統。

面對此重大資安威脅，GTIG 和 Mandiant 建議採取以下防護措施：

1. 立即套用Oracle官方發布的緊急修補程式，以修補CVE-2025-61882漏洞，防止攻擊者利用該漏洞進行遠端程式碼執行
2. 建議系統管理員定期檢查EBS資料庫，留意是否有異常資料或存取行為，因攻擊者可能將惡意酬載(payload)直接儲存於資料庫中
3. 阻斷所有從EBS伺服器向外網的非必要流量，限制伺服器與外部網路的通訊，降低潛在攻擊面
4. 持續監控並分析網路流量與系統日誌，儘早偵測任何可疑異常行為或攻擊跡象
5. 若懷疑系統已遭入侵，建議針對與EBS應用程式相關聯的Java行程進行記憶體分析，識別潛在惡意程式或異常活動

以下是Oracle提供的IoC：

200[.]107[.]207[.]26
185[.]181[.]60[.]11
76b6d36e04e367a2334c445b51e1ecce97e4c614e88dfb4f72b104ca0f31235d
aa0d3859d6633b62bccfb69017d33a8979a3be1f3f0a5a4bf6960d6c73d41121
6fd538e4a8e3493dda6f9fcdc96e814bdd14f3e2ef8aa46f0143bff34b882c1b

- 相關連結

1. Oracle Security Alert Advisory - CVE-2025-61882
2. Oracle E-Business Suite Zero-Day Exploited in Widespread Extortion Campaign
3. CrowdStrike Identifies Campaign Targeting Oracle E-Business Suite via Zero-Day Vulnerability
4. Well, Well, Well. It’s Another Day. (Oracle E-Business Suite Pre-Auth RCE Chain - CVE-2025-61882)
5. Oracle EBS Under Fire as Cl0p Exploits CVE-2025-61882 in Real-World Attacks
6. Apply Oracle Security Alert CVE-2025-61882 for Oracle E-Business Suite (EBS)

2.3 軟硬體漏洞資訊

2.3.1 Oracle E-Business Suite 存在重大資安漏洞(CVE-2025-61882)

CVE 編號	CVE-2025-61882
影響產品	Oracle E-Business Suite
解決辦法	根據官方網站釋出解決方式進行修補： https://www.oracle.com/security-s/-cve-2025-61882.html

- 內容說明：

  Oracle 發布重大資安漏洞公告(CVE-2025-61882，CVSS：9.8)，此漏洞存在於 Oracle E-Business Suite 的 Oracle Concurrent Processing，允許未經身分的攻擊者透過 HTTP 網路存取，可能導致遠端程式碼執行。

  備註：目前已觀察到有攻擊者利用此漏洞，建議儘速採取暫時緩解措施，以防止針對此漏洞可能的攻擊發生。

- 影響平台：
  - Oracle E-Business Suite 12.2.3-12.2.14
- 資料來源：
  1. Oracle Security Alert Advisory - CVE-2025-61882
  2. CVE-2025-61882

2.3.2 Veeam旗下Veeam Backup & Replication備份軟體存在2個重大資安漏洞

CVE 編號	CVE-2025-48983,CVE-2025-48984
影響產品	Veeam Backup & Replication
解決辦法	更新 Veeam Backup & Replication 12.3.2.4165 (含)之後版本

- 內容說明：

  Veeam Backup & Replication 是 Veeam 核心備份軟體，近日 Veeam 發布重大資安漏洞公告。

  【CVE-2025-48983，CVSS：9.9】

  此漏洞存在 Veeam Backup & Replication 的 Mount 服務中，允許經網域驗證的使用者，在備份基礎架構主機上執行遠端程式碼。

  【CVE-2025-48984，CVSS：9.9】

  此漏洞允許經網域驗證的使用者，在備份伺服器上執行遠端程式碼。

- 影響平台：
  - Veeam Backup & Replication 12.3.2.3617 (含)之前版本
- 資料來源：
  1. Vulnerabilities Resolved in Veeam Backup & Replication 12.3.2.4165 Patch

2.3.3 SAP 針對旗下Print Service修補重大資安漏洞(CVE-2025-42937)

CVE 編號	CVE-2025-42937
影響產品	SAP Print Service
解決辦法	請至官方網站進行修補： https://support.sap.com/en/my-support/knowledge-base/security-notes-news/october-2025.html

- 內容說明：

  SAP Print Service 是一項雲端列印解決方案，可將文件從雲端傳送至本地印表機，提供監控與管理列印追蹤功能。近期 SAP 月度更新公告，該服務存在 1 個重大資安漏洞(CVE-2025-42937，CVSS：9.8)，此漏洞源於對使用者提供的路徑資訊驗證不足，導致未經身分驗證的攻擊者，可以遍歷目錄並覆蓋系統文件。

- 影響平台：
  - SAPSPRINT 8.00、8.10 版本
- 資料來源：
  1. SAP Security Patch Day - October 2025
  2. CVE-2025-42937

2.3.4 SAP 針對旗下供應商關係管理系統修補重大資安漏洞(CVE-2025-42910)

CVE 編號	CVE-2025-42910
影響產品	SAP Supplier Relationship Management
解決辦法	請至官方網站進行修補： https://support.sap.com/en/my-support/knowledge-base/security-notes-news/october-2025.html

- 內容說明：

  SAP Supplier Relationship Management (SRM)是企業用來管理與供應商合作關係與優化的系統。近期 SAP 月度更新公告，該服務存在 1 個重大資安漏洞(CVE-2025-42910，CVSS：9.0)，此漏洞源於缺少文件類型或內容驗證，允許經過身分驗證的攻擊者上傳任意檔案，一旦被成功利用，攻擊者可能會對應用程式的機密性、完整性和可用性造成嚴重影響。

- 影響平台：
  - SRMNXP01 100、150 版本
- 資料來源：
  1. SAP Security Patch Day - October 2025
  2. CVE-2025-42910

2.3.5 Microsoft 旗下SharePoint Server 存在2個重大資安漏洞

CVE 編號	CVE-2025-59228,CVE-2025-59237
影響產品	Microsoft SharePoint Server
解決辦法	根據官方網站釋出解決方式進行修補： 【CVE-2025-59228】 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59228 【CVE-2025-59237】 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59237

- 內容說明：

  Microsoft SharePoint Server 是一款企業級協作平台，提供文件管理與團隊協作等功能，是企業資訊整合的核心平台。

  【CVE-2025-59228，CVSS：8.8】

  此為不正確輸入驗證漏洞，允許經授權的攻擊者透過網路執行程式碼。

  【CVE-2025-59237，CVSS：8.8】

  此為未受信任之資料反序列化漏洞，允許經授權的攻擊者透過網路執行程式碼。

- 影響平台：
  - Microsoft SharePoint Enterprise Server 2016
  - Microsoft SharePoint Server 2019
  - Microsoft SharePoint Server Subion Edition

- 資料來源：
  1. Microsoft SharePoint 遠端執行程式碼弱點
  2. CVE-2025-59228
  3. Microsoft SharePoint 遠端執行程式碼弱點
  4. CVE-2025-59237

2.3.6 Microsoft Exchange Server 存在重大資安漏洞(CVE-2025-59249)

CVE 編號	CVE-2025-59249
影響產品	Microsoft Exchange Server
解決辦法	根據官方網站釋出解決方式進行修補： https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59249

- 內容說明：

  微軟針對旗下產品 Exchange Server 發布重大資安漏洞公告(CVE-2025-59249，CVSS：8.8)，此漏洞為弱身分驗證漏洞，允許經授權的攻擊透過網路提升權限。

- 影響平台：
  - Microsoft Exchange Server Subion Edition RTM
  - Microsoft Exchange Server 2019 Cumulative Update 15
  - Microsoft Exchange Server 2019 Cumulative Update 14
  - Microsoft Exchange Server 2016 Cumulative Update 23
- 資料來源：
  1. Microsoft Exchange Server 權限提高弱點
  2. CVE-2025-59249

2.3.7 F5 的OS存在2個重大資安漏洞

CVE 編號	CVE-2025-57780,CVE-2025-61955
影響產品	F5OS
解決辦法	請更新至以下版本： F5OS - Appliance 1.8.3 版本 F5OS - Appliance 1.5.4 版本 F5OS - Chassis 1.8.2 版本 F5OS - Chassis 1.6.4 版本

- 內容說明：

  近日多雲應用服務和安全廠商 F5 發布 2 個重大資安漏洞(CVE-2025-57780，CVSS 3.x：8.8 和 CVE-2025-61955，CVSS：8.8)，皆為允許經過驗證且擁有本地存取權限的攻擊者提升權限，進而執行任意系統命令。

- 影響平台：
  - F5OS - Appliance 1.8.0
  - F5OS - Appliance 1.5.1 至 1.5.3 版本
  - F5OS - Chassis 1.8.0 至 1.8.1 版本
  - F5OS - Chassis 1.6.0 至 1.6.2 版本
- 資料來源：
  1. K000156771: F5OS vulnerability CVE-2025-57780
  2. CVE-2025-57780
  3. K000156767: F5OS vulnerability CVE-2025-61955
  4. CVE-2025-61955

第 3 章、資安研討會及活動

- **資安研討會**

2025 台灣資安通報應變年會：打造安全產品 串聯信任防線	
活動時間	**2025年12月03日 星期三**
活動地點	**臺大醫院國際會議中心 301廳(台北市中正區徐州路2號3樓)**
活動網站	**https://activity.twcert.org.tw/2025/index.htm**
活動概要	**【費用】** 免費 **【活動形式】** 實體與線上混合型會議(會場座席有限，開放TWCERT/CC會員優先參與且額滿為止) **【參加對象】** 國內各大企業、中小企業經營者、製造業者、高科技產業、資安領域相關業者、CERT/CSIRT組織、ISAC組織、SOC組織與對資安主題有興趣之單位。 **【活動內容 / Event Deails】** TWCERT/CC 主辦之台灣資安通報應變年會邁入第九屆，本次年會以「打造安全產品 串聯信任防線」為主題，聚焦資安趨勢與通報應變，從 AI 驅動下的新興威脅、台灣通報協調機制的成果與挑戰，到如何將通報落實為有效應變；進一步探討產品資安實務，從 Secure-by-Design 設計理念、PSIRT 弱點通報到供應鏈協作，剖析產品安全與品牌信任間的緊密關聯。期盼透過經驗交流與趨勢分享，強化企業與組織對資安通報、聯防協作及產品資安治理的實戰能力，打造更具韌性的資安生態。

	【指導單位】數位發展部 【主辦單位】數位發展部資通安全署、台灣電腦網路危機處理暨協調中心（TWCERT/CC） 【承辦單位】國家資通安全研究院 【報名洽詢】02-8729-1099#211 吳小姐 Evelyn.Wu@taiwan.messefrankfurt.com

第 4 章、TVN 漏洞公告

TWCERT/CC 本月份發布之CVSS 3.1分數為8.8以上之漏洞資訊如下表：

桓基科技｜iSherlock - OS Command Injection	
TVN / CVE ID	TVN-202510005 / CVE-2025-11900
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	影響產品： iSherlock 4.5 與 iSherlock 5.5 (包含 MailSherlock, SpamSherlock, AuditSherlock) 影響套件： iSherlock-smtp-4.5: 774(不含) 以前版本 iSherlock-smtp-5.5: 774(不含) 以前版本 iSherlock-base-4.5: 440(不含) 以前版本 iSherlock-base-5.5: 440(不含) 以前版本
問題描述	桓基科技開發之iSherlock存在OS Command Injection漏洞，未經身分鑑別之遠端攻擊者可注入任意作業系統指令並於伺服器上執行。
解決方法	更新 iSherlock-smtp-4.5 套件至 774(含)以後版本 更新 iSherlock-smtp-5.5 套件至 774(含)以後版本 更新 iSherlock-base-4.5 套件至 440(含)以後版本 更新 iSherlock-base-5.5 套件至 440(含)以後版本
公開日期	2025-10-17
相關連結	**https://www.twcert.org.tw/tw/cp-132-10440-dd55d-1.html**

傑印資訊｜筆硯公文管理系統 - Arbitrary File Upload	
TVN / CVE ID	TVN-202510006 / CVE-2025-11948
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	筆硯公文管理系統
問題描述	傑印資訊開發之筆硯公文管理系統存在Arbitrary File Upload漏洞，未經身分鑑別之遠端攻擊者可上傳並執行網頁後門程式，進而於伺服器端執行任意程式碼。
解決方法	請聯繫廠商進行更新
公開日期	2025-10-20
相關連結	**https://www.twcert.org.tw/tw/cp-132-10452-72cb6-1.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：**2025年10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/**