SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.10

https://stb.stpi.narl.org.tw/

資安暨智慧科技研發大樓

▶ 美國公布十大攸關資安的錯誤配置

美國國安局（National Security Agency，NSA）與國土安全部（DHS）旗下的網路安全暨基礎設施安全局（CISA）上周聯手公布了十大最常見的配置錯誤，這些錯誤的配置某種程度讓駭客更易展開攻擊，因而同時提出七項最佳安全作法以供軟體業者參考。

它們分別是軟體與應用程式的預設配置、使用者與管理員權限的分離不當、內部網路監控不足、缺乏網路分段、修補程式管理不善、繞過系統存取控制、多因素身分驗證薄弱或設定錯誤、網路共享與服務的存取控制名單不足、憑證衛生不佳，以及不受限的程式碼執行等。

【資料來源：iThome 2023.10.09】

▶ 中俄國家駭客涉嫌濫用WinRAR零時差漏洞

WinRAR編號CVE-2023-38831的漏洞遭駭客濫用，用以散布DarkMe等惡意程式。攻擊者可以製作惡意.ZIP或.RAR壓縮檔，當中包含無害檔案（例如.jpg、.txt或PDF檔等）及惡意執行檔，並以無害檔名為資料夾命名。當使用者點擊並試圖解壓縮看似合法的檔案時，即被安裝惡意程式。安全廠商偵測到，CVE-2023-38831最早從今年4月開始被濫用，針對加密貨幣交易用戶進行攻擊，旨在感染裝置取得交易平臺帳密，藉以竊取財物。

【資料來源：iThome 2023.10.19】

▶ 思科網路設備作業系統IOS XE的零時差漏洞已出現攻擊行動

思科揭露網路設備作業系統IOS XE的重大漏洞CVE-2023-20198，這項漏洞影響啟用網頁介面（Web UI），以及HTTP（或HTTPS）伺服器功能的網路設備，攻擊者若是成功利用該漏洞，就有機會在網路設備建立權限等級15的帳號，進而掌控整個系統，後續執行其他未經授權的惡意行動，CVSS風險評分為10。

【資料來源：資料來源：DARK READING 2023.10.17】

▶ 利用知名路由器漏洞傳播，Mirai DDoS 惡意軟體變種活躍

外媒報導Mirai 的 DDoS 惡意軟體僵屍網路變種 IZ1H9 近期開始活躍，鎖定知名廠牌 D-Link、Zyxel、TP-Link、TOTOLINK 路由器及 Linux 路由器。Fortinet 表示，9月第一周 IZ1H9惡意軟體針對易受攻擊設備的利用嘗試達到了數萬次。IZ1H9 在成功入侵受害者設備後，便將其加入 DDoS群組，然後對指定目標發起 DDoS 攻擊。Fortinet 表示IZ1H9使用多個2015 年到 2023 年路由器漏洞。

【資料來源：INFO SECURITY 2023.10.11】