SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.08.12 (六) —— 2023.08.18(五)

https://stb.stpi.narl.org.tw/
資安暨智慧科技研發大樓

TWCERT/CC首度舉辦企業資安演練，數位發展部領軍，邀來10家企業組隊參與

臺灣電腦網路危機處理暨協調中心（TWCERT/CC）於8月10日，首度舉辦「2023企業資安演練」，數位發展部、資安院組隊參與此次的演練活動，部長唐鳳也親自加入隊伍演練，以此彰顯政府對資安的重視，並邀請5家高科技公司日月光、台達電、合勤、華碩、啓碁科技，以及5大電信業者中華電信、台灣大哥大、遠傳電信、台灣之星、亞太電信參加，模擬駭客透過社交工程進行內部滲透，參演團隊需利用活動中提供之有限資訊，偵測駭客留下的軌跡，進行應變處理並阻斷攻擊，確保其資通系統持續營運不中斷。

【資料來源：iThome 2023.08.14】

警告：Zyxel 路由器五年前的漏洞仍在被利用

Fortinet 發出警告，Gafgyt 惡意軟體正積極利用 Zyxel P660HN-T1A 路由器五年前曝出的漏洞，每天發動數千次網路攻擊行動。據了解，漏洞編號為CVE-2017-18368，是路由器設備遠端系統日誌轉發功能中存在的嚴重性未驗證命令注入漏洞（CVSS v3：9.8分），Zyxel 已於 2017 年修補了該漏洞。2019 年時Zyxel 就強調當時的變種 Gafgyt惡意軟體可能會利用該漏洞發動攻擊，敦促仍在使用舊韌體版本的用戶儘快升級到最新版本，以保護其設備免遭攻擊接管。然而自 2023 年 7 月初以來，Fortinet 仍能夠監測到平均每天 7100 次的攻擊活動，且攻擊數量持續至今。為應對漏洞利用的爆發，Zyxel 又更新了安全公告，提醒客戶 CVE-2017-18363 只影響運行 7.3.15.0 v001/3.40(ULM.0)b31 或更舊韌體版本的設備，運行 2017 年為修復漏洞而推出的最新韌體版本 3.40(BYF.11) 的 P660HN-T1A 路由器不受影響。此外，Zyxel 表示 P660HN-T1A 在幾年前就已達到報廢年限。因此，強烈建議用戶汰換設備，以獲得最佳保護。

【資料來源：INFO SECURITY 2023.08.14】

SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.08.12 (六) —— 2023.08.18(五)

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

資安暨智慧科技研發大樓

中國駭客RedHotel針對包括臺灣在內的17個國家，進行為期3年的網路攻擊行動

長期觀察中國駭客行動的美國資安業者Recorded Future本周揭露，有一由中國政府支持的國家級駭客組織RedHotel，從2019年就開始滲透不同國家的政府及民間組織，特別是東南亞地區的國家，主要任務為情報蒐集及商業間諜，還會冒用其它組織的憑證與基礎設施來展開攻擊。RedHotel最值得一提的事蹟之一，就是在去年底盜走了一個屬於臺灣遊戲公司的程式簽章憑證，並簽署一個DLL以用來載入滲透測試工具Brute Ratel C4，此一工具可與越南國家級科學研究院的基礎設施進行通訊，顯示該越南組織也已被RedHotel攻陷，還被用來當作駭客的命令暨控制中心。此外，直至今年6月，RedHotel仍在使用越南教育及培訓部的TLS憑證。

【資料來源：iThome 2023.08.15】

近 2,000 台 Citrix NetScaler 伺服器在駭客的網路攻擊活動中被安裝了後門

資安公司Fox-IT（NCC 集團）和荷蘭漏洞揭露研究所(DIVD) 的安全研究人員發現了一項大規模的資安攻擊活動，此活動利用了編號為CVE-2023-3519且分類為嚴重等級的漏洞，此大規模的資安攻擊活動會在 Citrix Netscaler 伺服器上植入了 Webshell ，使得駭客可以擁有持久性的遠端存取權限 。儘管該漏洞已在7月18日發布更新程式，但顯然駭客的攻擊活動在更早的時侯已經展開。

【資料來源：BLEEPING COMPUTER 2023.08.15】