SHALUN
CYBER SECURITY HUB

資安週報

2022.09.24(五) —— 2022.09.30(五)

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

Sophos修補防火牆中的零時差漏洞

防毒軟體大廠Sophos發布了其防火牆產品的Patch更新，該漏洞編號為CVE-2022-3236 (CVSS 評分：9.8)，影響範圍為Sophos Firewall 19.0 MR1與之前的版本，該漏洞可能導致遠端程式碼執行，請產品使用者儘早更新產品至最新版本。

【資料來源：THEHACKERSNEWS, 2022.09.24】

駭客利用PowerPoint投影片模式散佈惡意軟體

威脅情報公司Cluster25指出，俄羅斯駭客組織APT28正在濫用PowerPoint投影片漏洞，只要受害者使用投影片模式，即使受害者未點擊連結，僅將滑鼠停留在連結上就可觸發含有惡意PowerShell的指令碼，並藉此散佈惡意軟體Graphite。

【資料來源：BLEEPINGCOMPUTER, 2022.09.26】

LockBit 3.0勒索軟體偽裝成求職者並發送電子郵件

近期LockBit 3.0勒索軟體偽裝成求職者的檔案並透過電子郵件發送求職訊息，它的攻擊對象很可能是針對公司。因此建議每家公司都必須將其反惡意軟體更新到最新版本，並加強其員工資安意識不要隨意開啟垃圾郵件內的信件。

【資料來源：ASEC, 2022.09.27】

針對Windows、Linux伺服器為目標的新型惡意軟體

使用Go語言編寫的惡意軟體Chaos正在快速傳播，它感染了廣泛的Linux和Windows設備，Chaos傳播的主要方式之一是利用已知漏洞，建議使用者定期重啟路由器並更新Patch，以及更改設備的預設密碼。

【資料來源： BLEEPINGCOMPUTER, 2022.09.28】