SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2022.12.03(六) —— 2022.12.09(五)

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

資安暨智慧科技研發大樓

嚴重的Ping漏洞允許駭客從遠端劫持FreeBSD系統

FreeBSD系統維護團隊已發布並更新Ping元件漏洞，該漏洞編號為CVE-2022-23093，影響範圍為所有的FreeBSD系統，一但駭客透過該漏洞進行攻擊，將有可能導致系統當機進而執行任意程式碼，由於此應用程式的處理程序會在相容模式沙箱運作，對於該作業系統的整體影響算是有限。

【資料來源： Thehackernews, 2022.12.05】

新的惡意軟體Zerobot利用21個漏洞入侵

Fortinet觀察到用Go語言編寫的殭屍網路Zerobot正在透過物聯網漏洞傳播，Zerobot可以掃描網路並自行傳播到相鄰的設備，也可以在Windows(CMD)或Linux(Bash)上執行命令，使用者需特別注意這種新的威脅，並在Patch可以更新時儘快更新Patch。

【資料來源： Fortinet, 2022.12.06】

Zombinder平台將惡意軟體綁定到合法的Android應用程式

Zombinder是一種新的混淆服務和犯罪平台，它允許駭客將惡意軟體綁定到合法的Android應用程式，這些應用程式能正常運行，因為它們原始的功能沒有被移除，之後Zombinder將惡意軟體載入到附加程式碼中以此混淆並逃避檢測，最終在後台執行。

【資料來源： BLEEPINGCOMPUTER, 2022.12.08】

使用通用攻擊方式繞過幾間供應商提供的WAF

Claroty的研究人員發現大部分的SQL引擎都支持JSON語法，並且默認啟用。於是研究人員使用JSON語法製作了一個新的SQL injection因為WAF在其SQL注入檢查過程中不支援JSON語法，這使JSON語法可以添加到SQL語句中，從而使WAF對惡意程式碼視而不見。

【資料來源：Securityweek, 2022.12.08】