SHALUN
CYBER SECURITY HUB

資安週報

2022.06.04 (六) —— 2022.06.10(五)

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

▶ 從word文件嵌入惡意檔案 “SVCReady”

研究人員在最近的網絡釣魚攻擊中發現了一種名為 “SVCReady” 的新惡意軟體。它以一種不尋常的方式將惡意軟體從Word文件載入到受感染的主機上。目前該惡意軟體已能達到資訊外洩、持續潛伏、反分析功能和加密的C2通訊。

【資料來源： BLEEPINGCOMPUTER, 2022.06.07】

▶ Linux核心權限提升漏洞 CVE-2022-32250

Linux核心版本5.18.1存在root權限提升漏洞，net/netfilter/nf_tables_api.c允許本地用戶（能夠新增用戶/網路名稱空間）並將權限提升到root，因為不正確的 NFT_STATEFUL_EXPR檢查會導致use-after-free。建議使用者立即更新Linux伺服器。

【資料來源： Penetration Testing, 2022.06.07】

▶ Black Basta 勒索軟體針對Linux伺服器上的VMware ESXi虛擬機

研究人員發現Black Basta變種勒索軟體針對 VMWare ESXi虛擬機進行加密。因為許多公司為了更容易管理設備及資源有效使用，所以大多數勒索軟體組織都將攻擊重點放在ESXi虛擬機上，除了可以利用單個命令對多個伺服器進行更快的加密外，這種策略也符合他們的企業目標。

【資料來源： BLEEPINGCOMPUTER, 2022.06.07】

▶ Owl Labs視訊會議設備的嚴重漏洞

研究人員在Owl Labs視訊會議設備Meeting Owl Pro中發現了五個漏洞：CVE-2022-31459、CVE-2022-31460、CVE-2022-31461（CVSS 7.4）、CVE-2022-31463（CVSS 8.2）和CVE-2022 -31462（CVSS 9.3），建議儘速更新到版本 5.4.1.4。 。

【資料來源： SECURITYWEEK, 2022.06.08】