2022/05/16~05/20 資安週報

NVIDIA修復十個Windows GPU顯示驅動中的漏洞

NVIDIA發布了針對各種顯卡型號的安全更新，此次更新解決了顯示卡驅動中的四個高危險漏洞(CVE-2022-28181、CVE-2022-28182、CVE-2022-28183、CVE-2022-28184)和六個中危險漏洞。建議產品使用者盡快進行安全更新。

【資料來源： BLEEPINGCOMPUTER, 2022.05.17】

駭客針對Tatsu WordPress外掛進行大規模攻擊

WordPress外掛Tatsu Builder存在遠程代碼執行漏洞CVE-2021-25094，其中大部分攻擊來自以下三個IP地址：148.251.183.254、176.9.117.218和217.160.145.62。建議將此IP加入黑名單並盡快將Tatsu WordPress外掛升級到3.3.1版本。

【資料來源：SecurityWeek, 2022.05.18 】

駭客攻擊Swagger-UI -從XSS到帳戶接管

Swagger UI存在DOM XSS的漏洞，雖然該漏洞已在2021年初修復。但是攻擊者仍能在許多公司中利用它，例如Paypal、Atlassian、Microsoft、GitLab、Yahoo等。

【資料來源：VIDOC Security Lab, 2022.05.16】

BlackByte勒索軟體團體正在打擊全球用戶

勒索軟體BlackByte 團體經常使用網路釣魚和未修補漏洞的應用程式或服務進行攻擊(例如易受攻擊的SonicWall VPN版本或Microsoft Exchange伺服器中的 ProxyShell漏洞)，如果您的公司正在使用Microsoft Exchange伺服器，請確保它始終維持最新更新。

【資料來源：Talos Intelligence, 2022.05.18】