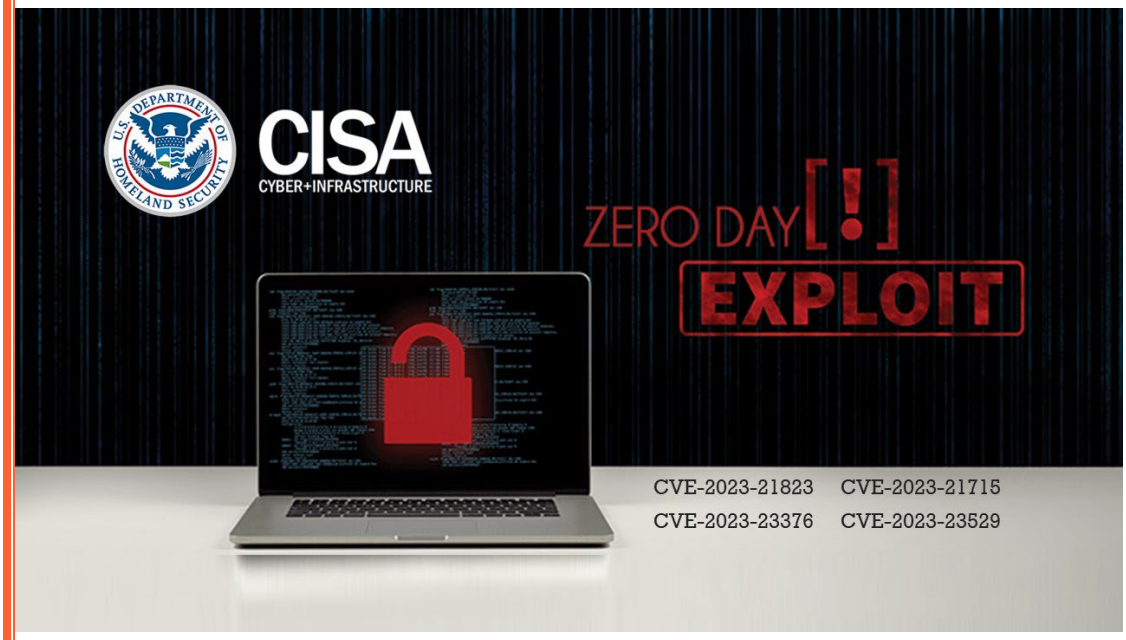
美國 CISA 警示 Windows 與 iOS 0-day 漏洞已遭用於資安攻擊



美國資安主管機關「網路安全暨基礎設施安全局」(Cybersecurity and Infrastructure Security Agency, CISA) 日前發表資安通報，公告有 4 個分別屬於 Windows 與 iOS 的 0-day 漏洞，由於設備採用數量眾多，目前已遭駭侵者用於攻擊行動；該告也通令美國聯邦各單位機關，須於三週內完成資安修補。

這次由 CISA 公告的 4 個 0-day 漏洞，前兩個是發生在 Microsoft Windows 系統中，其一 CVE-2023-21823 存於 WIndows Graphics Component，可用以遠端執行任意程式碼；其二 CVE-2023-23376 是存於 Windows Common Log File System Driver 中，駭侵者可藉以提升自身執行權限。

CISA 公告的第三個 0-day 漏洞 CVE-2023-21715 同樣針對 Microsoft 產品，是發生在 Microsoft Office 中的 Microsoft Publisher 中，屬於資安防護功能略過漏洞。而第四個 0-day 漏洞 CVE-2023-23529 則發生在 Apple iOS、iPadOS、macOS 中的

WebKit，是一種型別混淆漏洞，可用於執行任意程式碼。

發生在 Microsoft 產品的 3 個 0-day 漏洞，已在本月 Microsfot Patch Tuesday 資安修補包中修復；而 Apple iOS、iPadOS、macOS 的 0-day 漏洞也已推出更新版本予以修復。

根據公告於 2021 年 11 月的具約束力操作指引 (binding operational directive) BOD 22-01 規定，在 CISA 公布新的已遭用於攻擊漏洞時，所有美國聯邦政府民事機關，都必須針對相關漏洞進行處理。

關於本次公布的四個 0-day 漏洞，CISA 要求各機關須於三個星期內完成修補工作，最遲不可超過 2023 年 3 月 7 日。此外，雖然 CISA 的規定只生效於美國聯邦機關，但該單位強烈建議所有公私單位，都應該依照 CISA 的指引，立即修補漏洞，以免遭到攻擊。

建議各公私單位的系統管理員與個人用戶，都應隨時注意所用系統軟硬體的更新訊息，儘速更新到最新版本，以避免駭侵者利用未及時更新的已知漏洞發動攻擊。

(本文轉載自台灣電腦網路危機處理暨協調中心網站)