

張貼日期: 2024/12/17

【漏洞預警】中華電信 文件傳輸程式 - Reflected Cross-site Scripting to RCE

- 主旨說明: 中華電信 文件傳輸程式 - Reflected Cross-site Scripting to RCE
- 內容說明:
 - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202412-00000002
 - 【中華電信 文件傳輸程式 - Reflected Cross-site Scripting to RCE】(TVN-202412001) CVE-2024-12641 CVSS [9.6] 中華電信文件傳輸程式存在 Reflected Cross-site Scripting 漏洞。該程式會架設簡易本機端網站並提供 API 與標的網站溝通，由於 API 未對 CSRF 做防護，未經身分鑑別之遠端攻擊者可利用釣魚的方式使用特定 API 於使用者瀏覽器執行任意 JavaScript 程式碼。因該程式架設之網站支援 Node.js 特性，攻擊者可進一步利用達到執行任意作業系統指令。
- 影響平台: 文件傳輸程式 0.41.151 至 0.41.156 版本
- 建議措施: 更新文件傳輸程式至 0.41.157 (含) 以後版本
- 參考資料: <https://www.twcertorg.tw/tw/cp-132-8292-4fd98-1.html>

— 計算機與通訊中心
網路系統組 敬啟

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20241217_02

Last update: 2024/12/17 15:54