

張貼日期：2022/11/30

【資安漏洞預警】村榮資訊 雷電MAILD Mail Server 存在資安漏洞(CVE-2022-41675, CVE-2022-41676)

- 主旨說明：村榮資訊 雷電MAILD Mail Server 存在資安漏洞(CVE-2022-41675, CVE-2022-41676)

- 內容說明：

- 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-ANA-202211-0001
- 村榮資訊 雷電MAILD Mail Server 存在資安漏洞(CVE-2022-41675, CVE-2022-41676) 漏洞說明如下：
 - CVE-2022-41675雷電MAILD Mail Server網站的表單匯出功能未檢查所匯出的CSV檔案內容，遠端攻擊者以一般使用者權限登入後，可以將惡意程式注入到表單中，當其他使用者下載表單時，會取得惡意的CSV檔案，觸發任意程式碼執行，並對系統進行任意操作或中斷服務。
 - CVE-2022-41676雷電MAILD Mail Server網站的郵件欄位未過濾使用者輸入字串，遠端攻擊者以一般使用者權限登入後，在郵件欄位注入JavaScript語法並發送郵件，當受害者瀏覽郵件後，就會執行反射型XSS(Reflected Cross-site scripting)攻擊。

- 影響平台：

村榮資訊 雷電MAILD Mail Server v4.7

- 建議措施：

更新版本至v4.7.4以上

- 參考資料：

- <https://www.twcert.org.tw/tw/cp-132-6738-b78f4-1.html>
- <https://www.twcert.org.tw/tw/cp-132-6743-0a2c4-1.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:20221130_01

Last update: 2022/11/30 13:48