

張貼日期：2025/05/22

【漏洞預警】Fortinet 旗下多項產品存在重大資安漏洞(CVE-2025-32756)

- 主旨說明: 【漏洞預警】Fortinet 旗下多項產品存在重大資安漏洞(CVE-2025-32756)

- 內容說明:

- 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202505-00000016
- 近日Fortinet發布數項產品存在重大資安漏洞(CVE-2025-32756)【CVSS 9.8】影響範圍包含FortiVoice【FortiMail】FortiNDR【FortiRecorder 和 FortiCamera】此漏洞為堆疊溢位，允許未經身分驗證的遠端攻擊者利用精心設計的HTTP請求執行任意程式碼或命令。

- 影響平台:

- FortiCamera 2.1.0 至 2.1.3
- FortiCamera 2.0 所有版本
- FortiCamera 1.1 所有版本
- FortiMail 7.6.0 至 7.6.2
- FortiMail 7.4.0 至 7.4.4
- FortiMail 7.2.0 至 7.2.7
- FortiMail 7.0.0 至 7.0.8
- FortiNDR 7.6.0
- FortiNDR 7.4.0 至 7.4.7
- FortiNDR 7.2.0 至 7.2.4
- FortiNDR 7.1 所有版本
- FortiNDR 7.0.0 至 7.0.6
- FortiNDR 1.5 所有版本
- FortiNDR 1.4 所有版本
- FortiNDR 1.3 所有版本
- FortiNDR 1.2 所有版本
- FortiNDR 1.1 所有版本
- FortiRecorder 7.2.0 至 7.2.3
- FortiRecorder 7.0.0 至 7.0.5
- FortiRecorder 6.4.0 至 6.4.5
- FortiVoice 7.2.0
- FortiVoice 7.0.0 至 7.0.6
- FortiVoice 6.4.0 至 6.4.10

- 建議措施:

- 請更新至以下版本：
- FortiCamera 2.1.4(含)之後版本
- FortiMail 7.6.3(含)之後版本
- FortiMail 7.4.5(含)之後版本
- FortiMail 7.2.8(含)之後版本
- FortiMail 7.0.9(含)之後版本
- FortiNDR 7.6.1(含)之後版本
- FortiNDR 7.4.8(含)之後版本
- FortiNDR 7.2.5(含)之後版本
- FortiNDR 7.0.7(含)之後版本

- FortiRecorder 7.2.4(含)之後版本
 - FortiRecorder 7.0.6(含)之後版本
 - FortiRecorder 6.4.6(含)之後版本
 - FortiVoice 7.2.1(含)之後版本
 - FortiVoice 7.0.7(含)之後版本
 - FortiVoice 6.4.11(含)之後版本
 - 其餘未列出之產品版本，請遷移至固定版本
- 參考資料:
 - <https://www.twcert.org.tw/tw/cp-169-10127-ec862-1.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:20250522_01

Last update: **2025/05/22 11:12**

