

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2025040902045656	發佈時間	2025-04-09 14:28:56
事故類型	ANA-漏洞預警	發現時間	2025-04-09 14:21:56
影響等級	低		

[主旨說明:] **【漏洞預警】Fortinet 針對旗下 FortiSwitch 修補重大資安漏洞 (CVE-2024-48887)**

[內容說明:]

轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202504-00000005

FortiSwitch 是一款由 Fortinet 推出的乙太網路交換器，可與 FortiGate 防火牆整合，實現集中式簡化管理和智慧可擴展性。日前，Fortinet 發布 FortiSwitch GUI 存在重大資安漏洞(CVE-2024-48887，CVSS：9.8)並提出解決方案，此漏洞允許未經身分驗證的遠端攻擊者，透過精心設計的請求修改管理員密碼。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助公告或轉發

[影響平台:]

- FortiSwitch 6.4.0 至 6.4.14
- FortiSwitch 7.0.0 至 7.0.10
- FortiSwitch 7.2.0 至 7.2.8
- FortiSwitch 7.4.0 至 7.4.4

- FortiSwitch 7.6.0

[建議措施:]

更新至以下版本：

- FortiSwitch 6.4.15
- FortiSwitch 7.0.11
- FortiSwitch 7.2.9
- FortiSwitch 7.4.5
- FortiSwitch 7.6.1

[參考資料:]

1. <https://www.twcert.org.tw/tw/cp-169-10063-9de28-1.html>
2. <https://fortiguard.fortinet.com/psirt/FG-IR-24-435>
3. <https://nvd.nist.gov/vuln/detail/CVE-2024-48887>