

張貼日期：2025/07/02

【漏洞預警】CISA新增3個已知遭駭客利用之漏洞至KEV目錄(2025/06/23-2025/06/29)

- 主旨說明: 【漏洞預警】CISA新增3個已知遭駭客利用之漏洞至KEV目錄(2025/06/23-2025/06/29)
- 內容說明:
 - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202507-00000001
 - 1. CVE-2019-6693 Fortinet FortiOS Use of Hard-Coded Credentials Vulnerability (CVSS v3.1: 6.5)
 - 【是否遭勒索軟體利用:未知】 Fortinet FortiOS 存在使用硬體編碼憑證漏洞，攻擊者可藉由已知的硬體編碼金鑰，對FortiOS配置備份檔案中的敏感資料進行加解密操作。
 - 【影響平台】請參考官方所列的影響版本
 - <https://fortiguard.fortinet.com/psirt/FG-IR-19-007>
 - 2. CVE-2024-0769 D-Link DIR-859 Router Path Traversal Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用:未知】 D-Link DIR-859 路由器在其HTTP POST請求處理元件中的/hedwig.cgi檔案存在路徑遍歷漏洞，可能導致權限提升及未經授權控制裝置。
 - 【影響平台】請參考官方所列的影響版本
 - <https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10371>
 - 3. CVE-2024-54085 AMI MegaRAC SPx Authentication Bypass by Spoofing Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用:未知】 AMI MegaRAC SPx在Redfish主機介面中存在透過偽造達成的身份驗證繞過漏洞。成功利用此漏洞可能導致失去機密性、完整性及(或)可用性。
 - 【影響平台】請參考官方所列的影響版本
 - <https://www.ami.com/security-center/>
- 影響平台:
 - 詳細內容於內容說明欄之影響平台
- 建議措施:
 - 1. CVE-2019-6693 官方已針對漏洞釋出修復更新，請更新至相關版本
 - <https://fortiguard.fortinet.com/psirt/FG-IR-19-007>
 - 2. CVE-2024-0769 受影響的產品可能已經達到產品生命週期終點EoL和/或終止服務EoS建議使用者停止使用這些產品。
 - 3. CVE-2024-54085 官方已針對漏洞釋出修復更新，請更新至相關版本
 - <https://www.ami.com/security-center/>

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:20250702_02



Last update: **2025/07/02 11:26**