

張貼日期：2025/12/17

【漏洞預警】CISA新增7個已知遭駭客利用之漏洞至KEV目錄(2025/12/08-2025/12/14)

- 主旨說明: 【漏洞預警】CISA新增7個已知遭駭客利用之漏洞至KEV目錄(2025/12/08-2025/12/14)

- 內容說明:

- 轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-200-202512-00000007
- [CVE-2022-37055]D-Link Routers Buffer Overflow Vulnerability (CVSS v3.1: 9.8)
【是否遭勒索軟體利用:未知】D-Link 路由器存在緩衝區溢位漏洞，對機密性、完整性與可用性具有高度影響。受影響的產品可能已達生命週期終止[EoL]及 / 或服務終止[EoS]狀態，使用者應停止使用這些產品。
- [CVE-2025-66644]Array Networks ArrayOS AG OS Command Injection Vulnerability (CVSS v3.1: 7.2)
【是否遭勒索軟體利用:未知】Array Networks ArrayOS AG 存在作業系統指令注入漏洞，可能允許攻擊者執行任意指令。
- [CVE-2025-6218]RARLAB WinRAR Path Traversal Vulnerability (CVSS v3.1: 7.8)
【是否遭勒索軟體利用:未知】RARLAB WinRAR 存在路徑遍歷漏洞，允許攻擊者以當前使用者身分執行程式碼。
- [CVE-2025-62221]Microsoft Windows Use After Free Vulnerability (CVSS v3.1: 7.8)
【是否遭勒索軟體利用:未知】Microsoft Windows Cloud Files Mini Filter Driver 存在記憶體使用後釋放漏洞，可能允許已授權的攻擊者在本機提升權限。
- [CVE-2025-58360]OSGeo GeoServer Improper Restriction of XML External Entity Reference Vulnerability (CVSS v3.1: 8.2)
【是否遭勒索軟體利用:未知】OSGeo GeoServer 存在 XML 外部實體參照限制不當的漏洞，當應用程式接收 /geoserver/wms 端點 GetMap 操作的 XML 輸入時，可能允許攻擊者在 XML 請求中定義外部實體。
- [CVE-2018-4063]Sierra Wireless AirLink ALEOS Unrestricted Upload of File with Dangerous Type vulnerability (CVSS v3.1: 8.8)
【是否遭勒索軟體利用:未知】Sierra Wireless AirLink ALEOS 存在未受限制的危險類型檔案上傳漏洞。攻擊者可透過特製的 HTTP 請求上傳檔案，導致可執行程式碼被上傳至 Web 伺服器上，並可透過網路存取。攻擊者僅需發送已驗證的 HTTP 請求即可觸發此漏洞。受影響的產品可能已達生命週期終止[EoL]及 / 或服務終止[EoS]狀態，使用者應停止使用這些產品。
- [CVE-2025-14174]Google Chromium Out of Bounds Memory Access Vulnerability (CVSS v3.1: 8.8)
【是否遭勒索軟體利用:未知】Google Chromium 的 ANGLE 元件中存在越界記憶體存取漏洞，可能允許遠端攻擊者透過特製的 HTML 頁面執行越界記憶體存取。此漏洞可能影響多個使用 Chromium 的網頁瀏覽器，包括但不限於 Google Chrome、Microsoft Edge 與 Opera。

- 影響平台:

- [CVE-2022-37055]請參考官方所列的影響版本 <https://www.dlink.com/en/security-bulletin/>
- [CVE-2025-66644]ArrayOS AG 9.4.5.8(含)之前的版本

- [CVE-2025-6218] 請參考官方所列的影響版本
<https://www.win-rar.com/singlenewsview.html>
- [CVE-2025-62221] 請參考官方所列的影響版本
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62221>
- [CVE-2025-58360] 請參考官方所列的影響版本
<https://github.com/geoserver/geoserver/security/advisories/GHSA-fjf5-xgmq-5525>
- [CVE-2018-4063] Sierra Wireless AirLink ES450 FW 4.9.3
- [CVE-2025-14174] 請參考官方所列的影響版本
<https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#december-11-2025>
- 建議措施:
 - [CVE-2022-37055] 受影響的產品可能已達生命週期終止[EoL]及 / 或服務終止[EoS]狀態，使用者應停止使用這些產品。
 - [CVE-2025-66644] 對應產品升級至以下版本(或更高) ArrayOS AG 9.4.5.9
 - [CVE-2025-6218] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://www.win-rar.com/singlenewsview.html>
 - [CVE-2025-62221] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62221>
 - [CVE-2025-58360] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://github.com/geoserver/geoserver/security/advisories/GHSA-fjf5-xgmq-5525>
 - [CVE-2018-4063] 受影響的產品可能已達生命週期終止[EoL]及 / 或服務終止[EoS]狀態，使用者應停止使用這些產品。
 - [CVE-2025-14174] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#december-11-2025>

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:20251217_01

Last update: **2025/12/17 14:55**

