張貼日期：2025/11/05

【漏洞預警】CISA新增4個已知遭駭客利用之漏洞至KEV目錄(2025/10/27-2025/11/02)

- 主旨說明:【漏洞預警】CISA新增4個已知遭駭客利用之漏洞至KEV目錄(2025/10/27-2025/11/02)

- 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-200-202511-00000001
  1. 【CVE-2025-6204】Dassault Systèmes DELMIA Apriso Code Injection Vulnerability (CVSS v3.1: 8.0)
     - 【是否遭勒索軟體利用:未知】 Dassault Systèmes DELMIA Apriso 存在程式碼注入漏洞，可能允許攻擊者執行任意程式碼。
  2. 【CVE-2025-6205】Dassault Systèmes DELMIA Apriso Missing Authorization Vulnerability (CVSS v3.1: 9.1)
     - 【是否遭勒索軟體利用:未知】 Dassault Systèmes DELMIA Apriso 存在授權缺失漏洞，可能允許攻擊者取得對應程式的特權存取權限。
  3. 【CVE-2025-41244】Broadcom VMware Aria Operations and VMware Tools Privilege Defined with Unsafe Actions Vulnerability (CVSS v3.1: 7.8)
     - 【是否遭勒索軟體利用:未知】 Broadcom VMware Aria Operations 與 VMware Tools 存在本機權限提升漏洞。具非管理員權限的惡意本機使用者，若能存取已安裝 VMware Tools 且由 Aria Operations 管理並啟用 SDMP 的虛擬機，即可利用此漏洞在該虛擬機上將權限提升至 root】
  4. 【CVE-2025-24893】XWiki Platform Eval Injection Vulnerability (CVSS v3.1: 9.8)
     - 【是否遭勒索軟體利用:已知】 XWiki Platform 存在 eval 注入漏洞，可能允許任何訪客透過向 SolrSearch 發送請求來執行任意遠端程式碼。
- 影響平台:
  1. 【CVE-2025-6204】請參考官方所列的影響版本
     - https://www.3ds.com/trust-center/security/security-advisories/cve-2025-6204
  2. 【CVE-2025-6205】請參考官方所列的影響版本
     - https://www.3ds.com/trust-center/security/security-advisories/cve-2025-6205
  3. 【CVE-2025-41244】請參考官方所列的影響版本 https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149
  4. 【CVE-2025-24893】請參考官方所列的影響版本 https://jira.xwiki.org/browse/XWIKI-22149
- 建議措施:
  1. 【CVE-2025-6204】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://www.3ds.com/trust-center/security/security-advisories/cve-2025-6204
  2. 【CVE-2025-6205】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://www.3ds.com/trust-center/security/security-advisories/cve-2025-6205
  3. 【CVE-2025-41244】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149
  4. 【CVE-2025-24893】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://jira.xwiki.org/browse/XWIKI-22149

計算機與通訊中心
網路系統組 敬啟