Posted Date: 2025/11/05

[Vulnerability Alert] CISA Added 4 Known Exploited Vulnerabilities to KEV Catalog (2025/10/27-2025/11/02)

- Subject: [Vulnerability Alert] CISA Added 4 Known Exploited Vulnerabilities to KEV Catalog (2025/10/27-2025/11/02)
- Content:
    - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202511-00000001
    1. [CVE-2025-6204] Dassault Systèmes DELMIA Apriso Code Injection Vulnerability (CVSS v3.1: 8.0)
        - [Exploited by Ransomware: Unknown] Dassault Systèmes DELMIA Apriso has a code injection vulnerability, which may allow an attacker to execute arbitrary code.
    2. [CVE-2025-6205] Dassault Systèmes DELMIA Apriso Missing Authorization Vulnerability (CVSS v3.1: 9.1)
        - [Exploited by Ransomware: Unknown] Dassault Systèmes DELMIA Apriso has a missing authorization vulnerability, which may allow an attacker to obtain privileged access to the corresponding program.
    3. [CVE-2025-41244] Broadcom VMware Aria Operations and VMware Tools Privilege Defined with Unsafe Actions Vulnerability (CVSS v3.1: 7.8)
        - [Exploited by Ransomware: Unknown] Broadcom VMware Aria Operations and VMware Tools have a local privilege escalation vulnerability. A malicious local user with non-administrator privileges, who can access a virtual machine with VMware Tools installed, managed by Aria Operations, and with SDMP enabled, can exploit this vulnerability to escalate privileges to root on that virtual machine.
    4. [CVE-2025-24893] XWiki Platform Eval Injection Vulnerability (CVSS v3.1: 9.8)
        - [Exploited by Ransomware: Known] XWiki Platform has an eval injection vulnerability, which may allow any visitor to execute arbitrary remote code by sending a request to SolrSearch.
- Affected Platforms:
    1. [CVE-2025-6204] Please refer to the official listed affected versions
        - https://www.3ds.com/trust-center/security/security-advisories/cve-2025-6204
    2. [CVE-2025-6205] Please refer to the official listed affected versions
        - https://www.3ds.com/trust-center/security/security-advisories/cve-2025-6205
    3. [CVE-2025-41244] Please refer to the official listed affected versions https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149
    4. [CVE-2025-24893] Please refer to the official listed affected versions https://jira.xwiki.org/browse/XWIKI-22149
- Recommended Measures:
    1. [CVE-2025-6204] The official source has released a fix update for the vulnerability; please update to the relevant version https://www.3ds.com/trust-center/security/security-advisories/cve-2025-6204
    2. [CVE-2025-6205] The official source has released a fix update for the vulnerability; please update to the relevant version

   https://www.3ds.com/trust-center/security/security-advisories/cve-2025-6205

3. [CVE-2025-41244] The official source has released a fix update for the vulnerability; please update to the relevant version https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149
4. [CVE-2025-24893] The official source has released a fix update for the vulnerability; please update to the relevant version https://jira.xwiki.org/browse/XWIKI-22149

Computer and Communications Center
Network Systems Group

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20251105_03

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