مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Active Exploitation of Critical Vulnerabilities in DELMIA Apriso

Tracking #:432317873

Date:29-10-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed two newly identified vulnerabilities in Dassault Systèmes DELMIA Apriso, a key manufacturing execution system (MES) platform, have been exploited in the wild.

TECHNICAL DETAILS:

The flaws—CVE-2025-6204 (Code Injection) and CVE-2025-6205 (Missing Authorization)—impact DELMIA Apriso releases 2020 through 2025 and allow attackers to gain privileged access or execute arbitrary code remotely. These vulnerabilities pose a critical threat to manufacturing and industrial automation environments, with potential consequences including data theft, unauthorized system manipulation, and operational disruption.

Organizations using affected versions should prioritize immediate patching and network hardening to mitigate exploitation risks.

Vulnerability Details

1. **CVE-2025-6205** — Missing Authorization Vulnerability
   - CVSS v3.1 Score: 9.1 (CRITICAL)
   - Description: A missing authorization flaw in DELMIA Apriso (Releases 2020–2025) allows unauthenticated remote attackers to gain privileged access to sensitive components or administrative interfaces.
   - Impact: Attackers can perform unauthorized operations, modify system configurations, and access confidential data without authentication.
   - Exploitation Status: Observed exploited in the wild.
   - Affected Products: DELMIA Apriso Releases 2020–2025

2. **CVE-2025-6204** — Code Injection Vulnerability
   - CVSS v3.1 Score: 8.0 (HIGH)
   - Description: An Improper Control of Generation of Code (Code Injection) vulnerability allows authenticated attackers to inject and execute arbitrary code on the DELMIA Apriso application server.
   - Impact: Successful exploitation could lead to full system compromise, allowing attackers to alter production logic, deploy malicious payloads, or exfiltrate sensitive manufacturing data.
   - Exploitation Status: Observed exploited in the wild.
   - Affected Products: DELMIA Apriso Releases 2020–2025

RECOMMENDATIONS:

Apply Vendor Patches Immediately:

- Review Dassault Systèmes advisories and deploy all available security updates for DELMIA Apriso Releases 2020–2025.
- Implement vendor-provided mitigations if patches are pending.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.3ds.com/trust-center/security/security-advisories/cve-2025-6205
- https://www.3ds.com/trust-center/security/security-advisories/cve-2025-6204