

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Actively Exploited Vulnerability in DELMIA Apriso

Tracking #:432317700

Date:12-09-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that an actively exploited vulnerability has been identified in DELMIA Apriso, a platform used to manage manufacturing and supply-chain operations.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2025-5086) has been discovered in DELMIA Apriso, affecting releases from 2020 through 2025. The flaw, caused by deserialization of untrusted data, enables attackers to execute arbitrary code remotely on vulnerable systems.

Security researchers and threat intelligence reports confirm that this vulnerability is being actively exploited in the wild, significantly raising the risk to organizations that have not yet applied security updates. Successful exploitation could allow attackers to gain full control of affected application servers, disrupt production workflows, steal sensitive manufacturing data, or deploy malware within industrial networks.

Vulnerability Details:

- CVE ID: CVE-2025-5086
- Vulnerability Type: Deserialization of Untrusted Data
- Severity: Critical
- Exploitation Status: Actively Exploited in the Wild
- Impact: Remote Code Execution (RCE)
- Affected Product: DELMIA Apriso
- Affected Versions: Release 2020 through Release 2025

RECOMMENDATIONS:

- Immediately deploy official security patches or hotfixes for affected DELMIA Apriso versions.
- Remove direct internet exposure of DELMIA Apriso systems.
- Implement strict access controls and network segmentation.

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-2025-5086>