

CVE-2025-6204

Dassault Systèmes DELMIA Apriso Code Injection Vulnerability

CISA KEV since Oct 28, 2025

Actively exploited

An Improper Control of Generation of Code (Code Injection) vulnerability affecting DELMIA Apriso from Release 2020 through Release 2025 could allow an attacker to execute arbitrary code.

EVRS 82/₁₀₀ Urgent priority	CVSS V3.1 8.0 High · NVD	EPSS 0.792 99.6th percentile · FIRST	CISA DEADLINE Nov 18, 2025 CISA federal deadline · Overdue by 11 months
---	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.792 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
delmia apriso	≥ 2020 ≤ 2025	after 2025	NVD

Sources

Vendor guidance github.com/advisories/GHSA-xxh4-727v-gjcv

Additional guidance 3ds.com/trust-center/security/security-advisories/cve-2025-6204

NVD nvd.nist.gov/vuln/detail/CVE-2025-6204

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-23494

Current data evulnable.com/vulnerability-management/cve/CVE-2025-6204

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.