CISA Warns of DELMIA Apriso RCE Under Attack Impacting Automotive and Manufacturing

TL;DR

CISA confirmed active exploitation of CVE-2025-5086, a critical remote code execution flaw in Dassault DELMIA Apriso, software widely used in automotive and manufacturing environments.

Successful exploitation could disrupt production lines, resource planning, and supply chain operations. Federal agencies must patch by October 2, 2025.

Overview

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added CVE-2025-5086 to its Known Exploited Vulnerabilities catalog after confirming exploitation in the wild. The vulnerability, rated CVSS 9.0, affects all versions of DELMIA Apriso from Release 2020 through 2025.

Attackers are abusing a deserialization flaw to deliver malicious payloads via SOAP requests to Apriso endpoints. One payload was flagged as a Windows executable with malicious characteristics, and activity has been traced to IP address 156[.]244[.]33[.]162, likely tied to automated scans.

Automotive and manufacturing plants rely on DELMIA Apriso to keep production on schedule and manage resources. If attackers exploit this flaw, not only will assembly lines be halted, but data could be corrupted, and supply chains could be thrown off balance. Aspire recommends patching immediately.

Aspire Protects

- **Patch** – Apply Dassault's security updates immediately or discontinue use of vulnerable DELMIA Apriso versions (Releases 2020–2025).
- Monitor Apriso endpoints for unusual SOAP request activity.
- Review logs for traffic from 156[.]244[.]33[.]162 and investigate any suspicious behavior.
- This is not only a security issue but also a production risk.
- Federal agencies must patch by October 2, 2025, but private organizations should follow the same timeline.

TTPs to Watch

Execution

- Command and Scripting Interpreter [T1059] — The attacker may have executed malicious code by delivering a crafted payload through Apriso endpoints.

Persistence

- Boot or Logon Autostart Execution [T1547] – The attacker may have installed executables designed to maintain access across reboots.

Command and Control

- Application Layer Protocol [T1071] – The attacker may have used HTTP/S to communicate with infrastructure and deliver payloads.

Targeted Industries

This vulnerability directly impacts industries that depend on DELMIA Apriso to manage production and maintain strict process control:

- Automotive
- Aerospace
- Electronics
- High-Tech
- Industrial Machinery
- Manufacturing

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced

platform creates valuable context enabling end-to-end visibility across all threat vectors.
    - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
    - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
    - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

DELMIA Apriso - MOM Solutions | Dassault Systèmes

CVE-2025-5086 | Dassault Systèmes

Kaspersky Threats — Trojan.MSIL.Zapchast.gen

Exploit Attempts for Dassault DELMIA Apriso. CVE-2025-5086

CVE Record: CVE-2025-5086

CVE-2025-5086 – CISA