Public Exploit Released for Critical SAP NetWeaver Flaw - Against Invader

Data: 2025-08-20 23:24:43

Autor: Inteligência Against Invaders

A critical vulnerability in SAP NetWeaver AS Java Visual Composer, tracked as CVE-2025-31324, is

now being widely exploited following the release of public exploit tooling.

The flaw, patched in April 2025, allows unauthenticated remote code execution via the platform's metadata uploader endpoint.

What's new is the public availability of the full source code, which makes the exploit easy to use even for attackers with little technical expertise.

"With the source code now widely available, even script kiddies can leverage it,"said Jonathan Stross, SAP Security Analyst at Pathlock.

"The exploit is simple to execute – requiring only minutes to get running – and with AI tools like GPT, even inexperienced hackers could cause critical damage to organizations that remain unpatched."

Active Exploitation Confirmed

The US Cybersecurity & Infrastructure Security Agency (CISA) has recently added CVE-2025-31324 to its Known Exploited Vulnerabilities (KEV) catalog, highlighting its severity.

In fact, the flaw has been given a CVSS score of 10.0 by SAP's CNA and 9.8 by NVD, marking it as a top-priority threat.

"This new report from the Pathlock research team is a critical read for anyone in corporate cybersecurity,"said Frankie Sclafani, director of cybersecurity enablement at Deepwatch.

"It highlights how a vulnerability in SAP's NetWeaver Java Visual Composer, originally patched in April, is now being widely exploited."

Read more on SAP cybersecurity threats: SAP NetWeaver Flaw Exploited by Ransomware Groups and Chinese-Backed Hackers

Sclafani added: "This isn't just a hypothetical risk;CISA has already added this vulnerability […] to its [KEV] catalog. This confirms that real-world attacks are happening […] The bottom line is, if you're running this software and you haven't patched, you're at serious risk."

Pathlock also highlighted a related flaw, CVE-2025-42999, involving insecure deserialization, which has been chained with the uploader bug in attacks.

SAP addressed both issues in Security Notes 3594142 and 3604119.

Recommendations for Organizations

To reduce risk, Pathlock advises immediate action:

- Apply SAP Security Notes 3594142 and 3604119 across all Java instances
- Block or restrict access to the vulnerable /developmentserver/metadatauploader endpoint
- Hunt for signs of compromise using HTTP logs, servlet checks and SIEM alerts
- If compromised, isolate affected nodes, preserve evidence, rotate credentials and rebuild from a clean baseline

“NetWeaver is the web application where these products are hosted,”said Nivedita Murthy, senior staff consultant at Black Duck.

“This vulnerability is critical as it would allow attackers to laterally access other services without authentication and perform higher-level attacks.”