THREAT BULLETINS

Publicly Available Exploit Code Chains Critical SAP NetWeaver Flaws

TLP:WHITE

Aug 19, 2025

On August 15, 2025, exploit code was released that chains two critical vulnerabilities in SAP NetWeaver's Visual Composer to bypass authentication and achieve remote code execution.

The flaws, tracked as CVE-2025-31324 (CVSS score of 10) and CVE-2025-42999 (CVSS score of 9.1), are identified as a missing authorization check issue and an insecure deserialization bug, and were addressed in April and May, respectively.

Health-ISAC provides this information to increase situational awareness, encourage users to assess their level of risk to these vulnerabilities, and apply patches to affected instances.

SAP addressed the vulnerabilities in April and May 2025, following reports from security researchers who observed active exploitation. The first vulnerability, CVE-2025-31324, is a missing authorization check flaw that allows an unauthenticated attacker to upload arbitrary files to a vulnerable server. The second vulnerability, CVE-2025-42999, is an insecure deserialization flaw that can be exploited to achieve remote code execution.

The publicly available exploit confirms that attackers can not only deploy webshells but also live off the land by directly executing operating system commands without leaving artifacts. These commands run with SAP administrator privileges, granting full access to system resources and data.

Specifically, the exploit code allows threat actors to launch a two-step process attack that chains these vulnerabilities together to bypass security controls and gain full system control. In this attack, the attacker first exploits CVE-2025-31324 to upload a malicious payload to the SAP NetWeaver Visual Composer development server without needing any credentials. This initial step provides a foothold on the server. After completing the first stage, the attacker then exploits CVE-2025-42999 to execute the malicious payload with high privileges on the SAP system.

The public release of exploit code chaining the critical vulnerabilities poses an immediate threat, as these flaws were previously leveraged by ransomware groups like Qilin and BianLian, along with China-nexus espionage threat actors, to target critical infrastructure. SAP systems are often the backbone for managing critical business processes, supply chains, and sensitive data. A compromise of an SAP system could lead to the theft of confidential data, disruption of supply chains, and potential manipulation of business-critical information, which could lead to legal penalties and reputational damage.

Recommendations:

Health-ISAC recommends organizations review and assess their level of risk to these vulnerabilities and take the necessary steps to implement appropriate actions, including:

- Applying the latest security patches from SAP
- Reviewing and restricting access to SAP applications, especially from the Internet.
- Monitoring SAP applications for any signs of compromise, such as unexpected file uploads or unusual processes.
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	securityweek, thehackernews, x, onapsis, onapsis 1, nist, nist 1

Alert ID 0ce29084

View Alert

Share Feedback

was this helpful?  | 

Tags SAP NetWeaver Visual Composer, CVE-2025-42999, CVE-2025-31324

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.  

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.