

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

**Critical CVE-2025-31324 Flaw in SAP  
NetWeaver Under Active Attack**

Date of Publication

April 29, 2025

Admiralty Code

A1

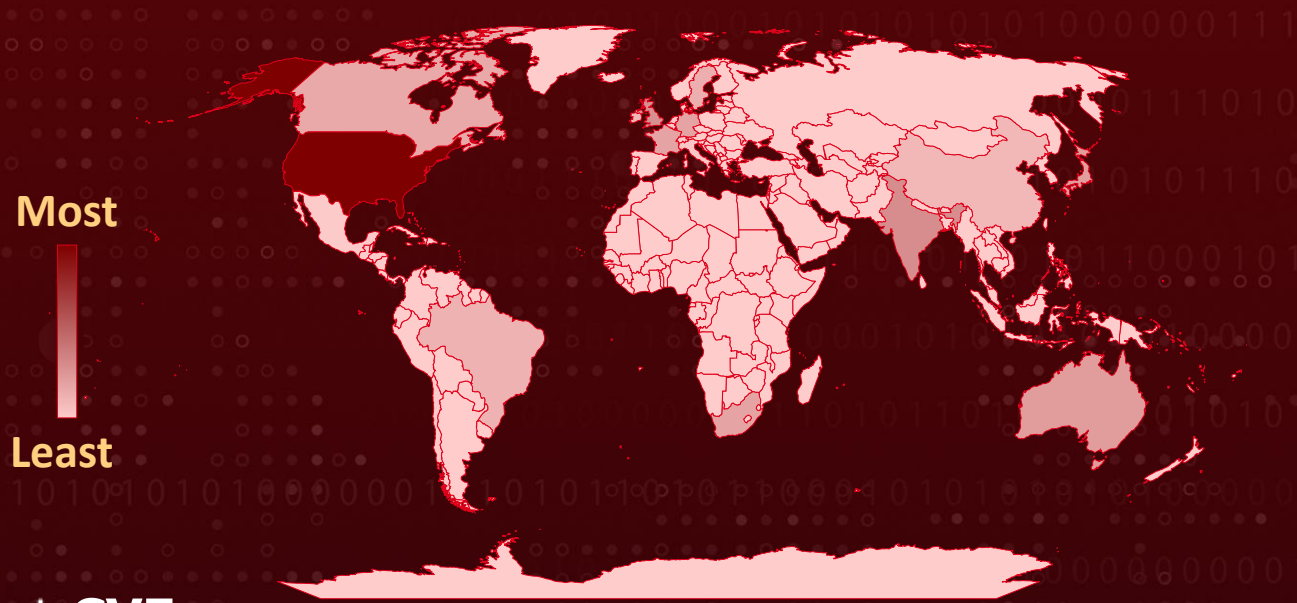
TA Number

TA2025131

# Summary

**First Seen:** March 27, 2025  
**Affected Products:** SAP NetWeaver  
**Targeted Regions:** Worldwide  
**Impact:** A critical zero-day flaw in SAP NetWeaver (CVE-2025-31324) is being actively exploited by attackers to drop web shells and run malicious code on vulnerable servers. By abusing a missing security check, threat actors can upload harmful files without logging in making this a serious risk to any unpatched system. Users of SAP NetWeaver, update immediately and lock down access to stay protected.

## 🔪 Targeted Regions



## ⚙️ CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-31324	SAP NetWeaver Unrestricted File Upload Vulnerability	SAP NetWeaver	✔️	✔️	✔️

# Vulnerability Details

## #1

SAP has addressed a critical zero-day flaw, tracked as CVE-2025-31324, in its NetWeaver Visual Composer platform. Rated with the maximum severity score of 10.0, the flaw is already being actively exploited in the wild. Attackers are using it to upload malicious files such as web shells and run unauthorized code on vulnerable servers without needing any authentication.

## #2

SAP NetWeaver is a key platform used by businesses to integrate data, processes, and applications across their infrastructure so a compromise here can have serious consequences. The vulnerability stems from a missing authorization check in the Metadata Uploader component. This allows attackers to send specially crafted POST requests to the `/developmentserver/metadatauploader` endpoint and upload harmful files directly to the system.

## #3

In observed attacks, threat actors have uploaded JSP-based web shells to the following directory: `"j2ee/cluster/apps/sap.com/irj/servlet_jsp/irj/root/"`. These web shells grant remote access to the attackers, enabling them to execute commands, upload additional tools, and maintain persistent control of the system. Attackers also leveraged advanced tools like Brute Ratel a post-exploitation framework used for process injection, privilege escalation, credential theft, and lateral movement and Heaven's Gate, which helps evade detection by switching between 32-bit and 64-bit execution modes during code execution.

## #4

If left unpatched, this flaw can lead to a full system compromise putting sensitive business data and critical operations at risk. All organizations are urged to immediately update NetWeaver to the latest version, without waiting for regular maintenance windows. Additionally, access to the vulnerable endpoint should be restricted, and systems should be scanned for signs of suspicious uploads or activity.

## #5

Current exploitation has been observed targeting a wide range of countries, including United States of America, India, United Kingdom of Great Britain and Northern Ireland, Australia, Japan. Organizations in these regions especially those heavily reliant on SAP systems should treat this vulnerability as a top priority.

# Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-31324	SAP NetWeaver Version 7.50	cpe:2.3:a:sap:sap_netweaver:7.50:*:*:*:*:*	CWE-434

## Recommendations



**Update Immediately:** Update SAP NetWeaver right away to fix the CVE-2025-31324 issue. Don't wait for your usual patch schedule this update is critical and should be handled as an emergency.



**Limit Access:** Limit who can reach the vulnerable endpoint at /developmentserver/metadatauploader. Block it from the internet, and if it must be used, make sure only trusted internal systems have access.



**Strengthen Web and Network Security Defenses:** Deploy web application firewalls (WAFs), intrusion detection/prevention systems (IDS/IPS), and enforce strict access controls to help detect and block unusual upload activity or unauthorized access attempts. In addition, configure your security tools to monitor for behaviors linked to advanced post-exploitation tools like Brute Ratel and Heaven's Gate such as process injection, in-memory payload execution, and thread manipulation so you can catch threats early and respond quickly.



**Vulnerability Management:** This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.



# Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>TA0003</u></b> Persistence
<b><u>TA0004</u></b> Privilege Escalation	<b><u>TA0005</u></b> Defense Evasion	<b><u>TA0011</u></b> Command and Control	<b><u>T1588</u></b> Obtain Capabilities
<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1505</u></b> Server Software Component	<b><u>T1505.003</u></b> Web Shell
<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1068</u></b> Exploitation for Privilege Escalation	<b><u>T1562</u></b> Impair Defenses	<b><u>T1071</u></b> Application Layer Protocol
<b><u>T1566</u></b> Phishing	<b><u>T1566.001</u></b> Spearphishing Attachment		

## Indicators of Compromise (IOCs)

TYPE	VALUE
<b>SHA256</b>	1f72bd2643995fab4ecf7150b6367fa1b3fab17afd2abed30a98f075e4913087, 794cb0a92f51e1387a6b316b8b5ff83d33a51ecf9bf7cc8e88a619ecb64f1dcf, b3e4c4018f2d18ec93a62f59b5f7341321aff70d08812a4839b762ad3ade74ee

## Patch Details

Update SAP NetWeaver to the latest version.

Link: <https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html>

## References

<https://reliquest.com/blog/threat-spotlight-reliquest-uncovers-vulnerability-behind-sap-netweaver-compromise/>

<https://onapsis.com/blog/active-exploitation-of-sap-vulnerability-cve-2025-31324/>

[https://github.com/redrays-io/CVE-2025-31324/blob/main/Scanner\\_CVE-2025-31324.py](https://github.com/redrays-io/CVE-2025-31324/blob/main/Scanner_CVE-2025-31324.py)

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON  
**April 29, 2025 • 5:50 AM**

© 2025 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)