Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

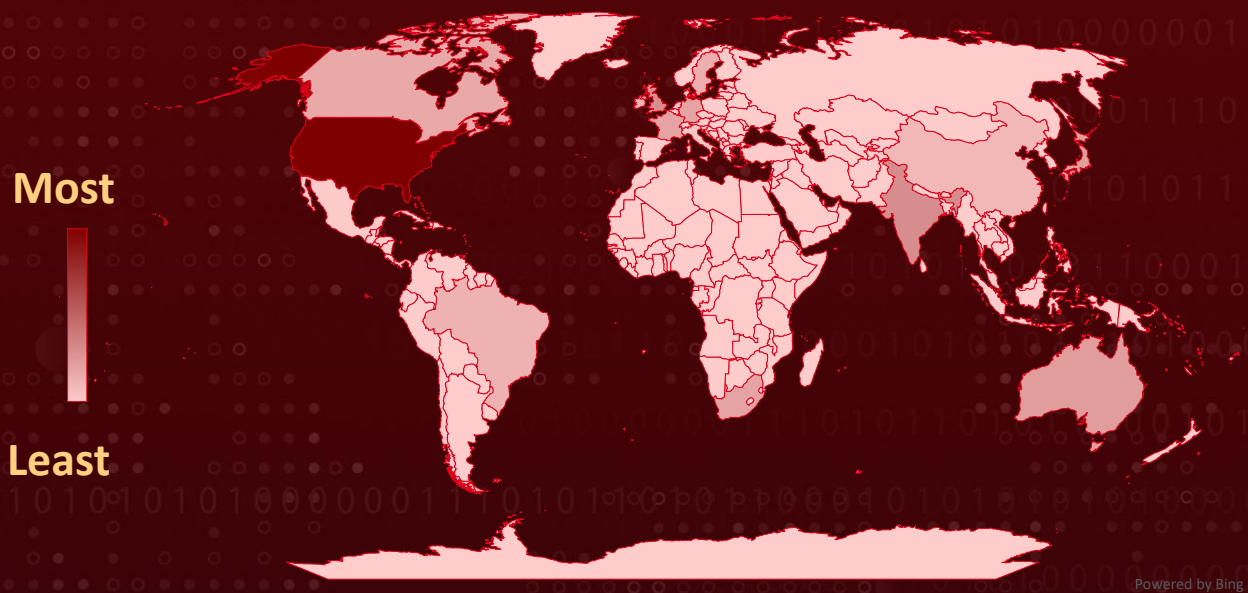
Critical CVE-2025-31324 Flaw in SAP NetWeaver Under Active Attack

Date of Publication	Last Update Date	Admiralty Code	TA Number
April 29, 2025	June 4, 2025	A1	TA2025131

Summary

First Seen: March 27, 2025
Affected Products: SAP NetWeaver
Actor: UNC5221, UNC5174, CL-STA-0048
Malware: KrustyLoader, Qilin ransomware, BianLian, RansomExx, PipeMagic
Targeted Regions: Worldwide
Targeted Industries: Government, Finance, Oil and Gas
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



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-31324	SAP NetWeaver Unrestricted File Upload Vulnerability	SAP NetWeaver	✓	✓	✓
CVE-2025-42999	SAP NetWeaver Deserialization 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. 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.

#5 Recent findings reveal that several cybercriminal groups, including the Russian ransomware gang BianLian and the operators behind RansomEXX, are showing active interest in exploiting this vulnerability. This growing trend underscores how threat actors are racing to weaponize such flaws for financial gain. These two ransomwares are exploiting the flaw to deploy PipeMagic.

#6 Meanwhile, Chinese state-linked hacking groups like UNC5221, UNC5174, and CL-STA-0048 have been found exploiting CVE-2025-31324 to plant a variety of malicious payloads on vulnerable SAP NetWeaver systems. Each group follows distinctive attack patterns.

#7 To make matters more concerning, a separate investigation revealed that attackers associated with the Qilin ransomware group began exploiting CVE-2025-31324 along with a related bug, CVE-2025-42999 at least three weeks before the vulnerabilities were publicly disclosed. This highlights just how fast threat actors move once a weakness is discovered, often outpacing public awareness and defenses.

Vulnerabilities

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
CVE-2025-42999	SAP NetWeaver Java systems Version 7.1x and above	cpe:2.3:a:sap:netweaver:7.5:*:*:*:*:*:*:*	CWE-502

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

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**TA0005** Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery
TA0008 Lateral Movement	**TA0010** Exfiltration	**TA0011** Command and Control	**TA0040** Impact
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1190** Exploit Public-Facing Application	**T1505** Server Software Component
T1505.003 Web Shell	**T1059** Command and Scripting Interpreter	**T1059.006** Python	**T1059.007** JavaScript
T1071 Application Layer Protocol	**T1566** Phishing	**T1566.001** Spearphishing Attachment	**T1068** Exploitation for Privilege Escalation
T1562 Impair Defenses	**T1203** Exploitation for Client Execution	**T1547** Boot or Logon Autostart Execution	**T1547.006** Kernel Modules and Extensions
T1140 Deobfuscate/Decode Files or Information	**T1027** Obfuscated Files or Information	**T1003** OS Credential Dumping	**T1003.008** /etc/passwd and /etc/shadow
T1087 Account Discovery	**T1010** Application Window Discovery	**T1580** Cloud Infrastructure Discovery	**T1526** Cloud Service Discovery

T1210 Exploitation of Remote Services	**T1041** Exfiltration Over C2 Channel	**T1486** Data Encrypted for Impact	**T1105** Ingress Tool Transfer

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1f72bd2643995fab4ecf7150b6367fa1b3fab17afd2abed30a98f075e4913087, 794cb0a92f51e1387a6b316b8b5ff83d33a51ecf9bf7cc8e88a619ecb64f1dcf, b3e4c4018f2d18ec93a62f59b5f7341321aff70d08812a4839b762ad3ade74ee, 0a866f60537e9decc2d32cbdc7e4dcef9c5929b84f1b26b776d9c2a307c7e36e, 4d4f6ea7ebdc0fbf237a7e385885d51434fd2e115d6ea62baa218073729f5249, 1579b6776eeaf79cbd0852fa9cdb3656e16688ca65e7806c9bc018eefebe0ae8, 565d7ed059e2d60fa69cc51a6548aa9f8192a71f4cd79112823f3f628cfede85, ec30c87f65f16e3b591e7ce74229a700c59766e242be3df46979fea54c330873, 31d7d0dab2fb367c24be0b1a08a7b751d2967f3999307f217d9230ea485a3743, a5818e3a58198da5b8ea4cc001a7cecf06aa8a7684489743976996b8cddbd200, 4c9e60cc73e87da4cadc51523690d67549de4902e880974bfacf7f1a8dc40d7d, 63aa0c6890ec5c16b872fb6d070556447cd707dfba185d32a2c10c008dbdbcdd, f92d0cf4d577c68aa615797d1704f40b14810d98b48834b241dd5c9963e113ec, 47ff0ae9220a09bfad2a2fb1e2fa2c8ffe5e9cb0466646e2a940ac2e0cf55d04, 3f14dc65cc9e35989857dc1ec4bb1179ab05457f2238e917b698edb4c57ae7ce, 91f66ba1ad49d3062afdcc80e54da0807207d80a1b539edcdbd6e1bf99e7a2ca, c71da1dfea145798f881afd73b597336d87f18f8fd8f9a7f524c6749a5c664e4, b8e56de3792dbd0f4239b54cfaad7ece3bd42affa4fbbdd7668492de548b5df8,

TYPE	VALUE
SHA256	0c2c8280701706e0772cb9be83502096e94ad4d9c21d576db0bc627e1e84b579, 5f3d1f17033d85b85f3bd5ae55cb720e53b31f1679d52986c8d635fd1ce0c08a, 2dcbb4138f836bb5d7bc7d8101d3004848c541df6af997246d4b2a252f29d51a, 00920e109f16fe61092e70fca68a5219ade6d42b427e895202f628b467a3d22e, b9533ce8e428f16f3d0e1946f19a6f756ff11a532d0b7e61ae402837f46c678e, 888e953538ff668104f838120bc4d801c41adb07027db16281402a62f6ec29ef, 5e24b41a0bd076ec2b4e49e66daac94396c6180d00a45bcd7f4342a385fa1eed
Domains	dns[.]telemetrymasterhostname[.]com, aaa[.]ki6zmfw3ps8q14rfbfczfq5qkhq8e12q[.]oastify[.]com, applr-malbbal[.]s3[.]ap-northeast-2[.]amazonaws[.]com, abode-dashboard-media[.]s3[.]ap-south-1[.]amazonaws[.]com, brandnav-cms-storage[.]s3[.]amazonaws[.]com, ocr-freespace[.]oss-cn-beijing[.]aliyuncs[.]com/2025/config[.]sh
MD5	D1C43F8DB230BDF18C61D672440EBA12, 6914B1F5B6843341FAFDFAA9D57818B9
URL	hxxp[:]//184[.]174[.]96[.]70/rs64c[.]exe, hxxp[:]//184[.]174[.]96[.]74/rs64c[.]exe
Path	\usr\sap\PP1\J01\j2ee\cluster\apps\sap.com\irj\servlet_jsp\irj\root\
File Names	random12.jsp, duchyofn.jsp, rbekqaun.jsp, rwlrqhrj.jsp, xxkmszdm.jsp, gpfmddkh.jsp, bdtzvjzm.jsp, decoxfiv.jsp, zdulvrqu.jsp, ran_new.jsp, JEE_jsp_bdtzvjzm_1743883325986.class, test.exe, ESC.exe
IPv4	184[.]174[.]96[.]74, 184[.]174[.]96[.]70, 180[.]131[.]145[.]73, 43[.]247[.]135[.]53,

TYPE	VALUE
IPv4	54[.]77[.]139[.]23 3[.]248[.]33[.]252, 103[.]30[.]76[.]206, 45[.]155[.]222[.]14, 15[.]204[.]56[.]106, 159[.]65[.]34[.]242, 138[.]68[.]61[.]82 192[.]243[.]115[.]175, 107[.]175[.]77[.]118, 15[.]188[.]246[.]198, 138[.]197[.]40[.]133, 43[.]247[.]135[.]53, 23[.]95[.]123[.]5, 215[.]204[.]56[.]106, 27[.]25[.]148[.]183, 65[.]20[.]81[.]172, 3[.]125[.]102[.]39, 212[.]11[.]64[.]225, 130[.]185[.]118[.]247, 212[.]192[.]15[.]213, 52[.]172[.]31[.]130, 149[.]62[.]46[.]132, 196[.]251[.]85[.]31, 162[.]248[.]53[.]119, 103[.]30[.]76[.]206, 206[.]237[.]1[.]201, 141[.]164[.]35[.]53, 107[.]174[.]81[.]24, 208[.]76[.]55[.]39, 52[.]185[.]157[.]28, 65[.]49[.]235[.]210, 185[.]143[.]222[.]215, 185[.]165[.]169[.]31, 46[.]29[.]161[.]198, 62[.]234[.]24[.]38, 64[.]233[.]180[.]99, 45[.]77[.]119[.]13, 23[.]227[.]196[.]204, 184[.]174[.]96[.]39, 96[.]9[.]124[.]89, 156[.]238[.]224[.]227, 153[.]92[.]4[.]236, 45[.]61[.]137[.]162, 64[.]95[.]11[.]95, 142[.]202[.]4[.]28, 154[.]37[.]221[.]237

TYPE	VALUE
IPv4	50[.]114[.]94[.]55, 63[.]135[.]161[.]223, 199[.]101[.]196[.]85, 212[.]30[.]36[.]232, 50[.]114[.]94[.]56, 63[.]135[.]161[.]224, 212[.]30[.]36[.]171, 212[.]30[.]36[.]234, 50[.]114[.]94[.]57, 63[.]135[.]161[.]226, 212[.]30[.]36[.]173, 216[.]73[.]161[.]8, 50[.]114[.]94[.]68, 63[.]135[.]161[.]229, 212[.]30[.]36[.]175, 216[.]73[.]161[.]15, 50[.]114[.]94[.]72, 63[.]135[.]161[.]235, 212[.]30[.]36[.]176, 216[.]73[.]161[.]17, 50[.]114[.]94[.]74, 63[.]135[.]161[.]242, 212[.]30[.]36[.]183, 216[.]73[.]161[.]18, 50[.]114[.]94[.]86, 63[.]135[.]161[.]245, 212[.]30[.]36[.]200, 216[.]73[.]161[.]20, 50[.]114[.]94[.]91, 85[.]239[.]54[.]153, 212[.]30[.]36[.]206, 216[.]73[.]161[.]21, 50[.]114[.]94[.]95, 91[.]193[.]19[.]36, 212[.]30[.]36[.]215, 216[.]73[.]161[.]22, 50[.]114[.]94[.]97, 142[.]111[.]152[.]19, 212[.]30[.]36[.]218, 216[.]73[.]161[.]25, 50[.]114[.]94[.]100, 142[.]111[.]152[.]20, 212[.]30[.]36[.]219, 216[.]73[.]161[.]26, 50[.]114[.]94[.]104, 142[.]111[.]152[.]23,

TYPE	VALUE
IPv4	212[.]30[.]36[.]228, 63[.]135[.]161[.]220, 142[.]111[.]152[.]24, 212[.]30[.]36[.]231, 91[.]193[.]19[.]36, 143[.]198[.]173[.]194, 136[.]144[.]35[.]192, 136[.]144[.]35[.]206, 91[.]218[.]50[.]174, 167[.]99[.]150[.]59, 136[.]144[.]35[.]196, 136[.]144[.]35[.]207, 206[.]189[.]229[.]132, 37[.]49[.]228[.]122, 136[.]144[.]35[.]197, 136[.]144[.]35[.]213, 159[.]89[.]93[.]5, 206[.]188[.]197[.]52, 136[.]144[.]35[.]199, 89[.]187[.]164[.]96, 104[.]248[.]236[.]95, 85[.]239[.]54[.]153, 136[.]144[.]35[.]200, 136[.]144[.]35[.]210, 142[.]93[.]63[.]24, 192[.]42[.]116[.]200, 136[.]144[.]35[.]201, 136[.]144[.]35[.]211, 134[.]122[.]26[.]60, 103[.]207[.]14[.]236, 136[.]144[.]35[.]202, 136[.]144[.]35[.]189, 137[.]184[.]197[.]225, 104[.]28[.]212[.]150, 136[.]144[.]35[.]203, 136[.]144[.]35[.]214, 167[.]99[.]11[.]36, 104[.]28[.]244[.]150, 136[.]144[.]35[.]204, 204[.]48[.]22[.]207, 136[.]144[.]35[.]191, 136[.]144[.]35[.]205

Patch Details

Update SAP NetWeaver to the latest version.

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

References

https://reliaquest.com/blog/threat-spotlight-reliaquest-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

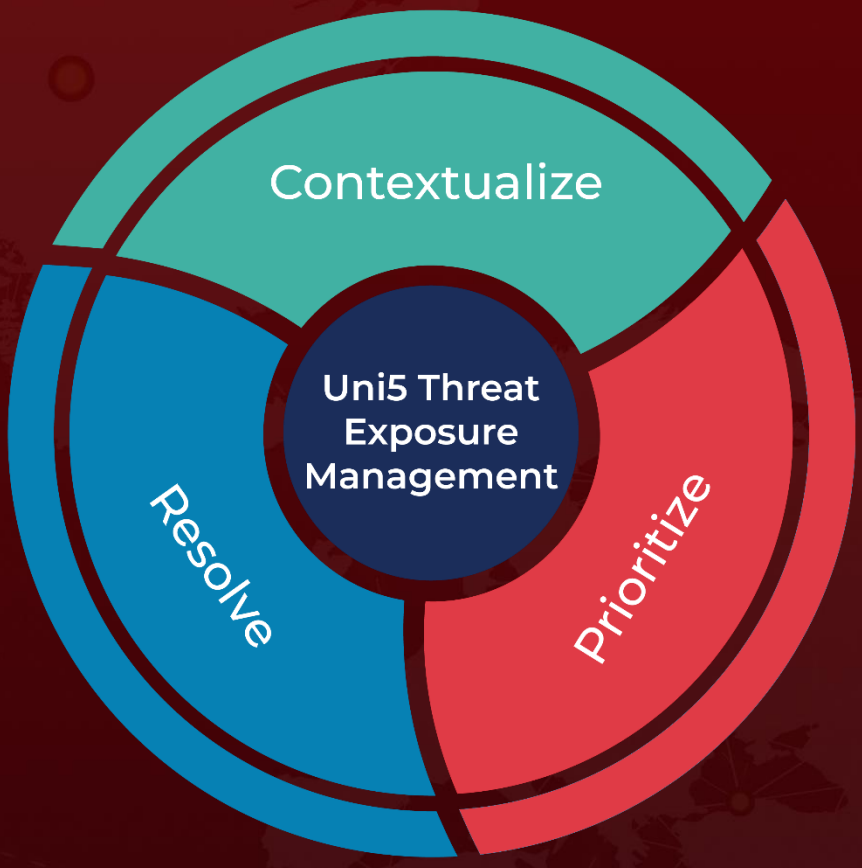
https://blog.eclecticiq.com/china-nexus-nation-state-actors-exploit-sap-netweaver-cve-2025-31324-to-target-critical-infrastructures

https://op-c.net/blog/sap-cve-2025-31324-qilin-breach/?utm_campaign=li-sapzero&utm_source=linkedin&utm_medium=organic

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