SAP Vulnerability in the Wild by Chinese Threat Actor

forescout.com/blog/threat-analysis-sap-vulnerability-exploited-in-the-wild-by-chinese-threat-actor/

May 8, 2025

Key Findings

- CVE-2025-31324 affecting SAP NetWeaver Visual Composer is being actively exploited in the wild.
- We uncovered new malicious infrastructure belonging to a Chinese threat actor exploiting this CVE.

Mitigation Recommendations

- Apply SAP patches immediately
- Restrict access to metadata uploader services
- Disable Unused web services – If the Visual Composer service is non-essential, consider disabling it entirely.
- Monitor for abnormal access or changes to service entries, especially outside of maintenance windows.

CVE-2025-31324 is a critical deserialization vulnerability affecting SAP NetWeaver Visual Composer 7.x that allows attackers to upload malicious binaries, such as web shells to vulnerable servers. This allows for full takeover of unpatched systems.

The CVE is actively being exploited in the wild since at least April 29, when we noticed active scans on Forescout's Adversary Engagement Environment (AEE) and it was added to CISA KEV.

As part of our investigation into active exploitation of this vulnerability, we uncovered malicious infrastructure likely belonging to a Chinese threat actor, which we are currently tracking as Chaya_004 – following our convention for unnamed threat actors. The infrastructure includes a network of servers hosting Supershell backdoors, often deployed on Chinese cloud providers, and various pen testing tools, many of Chinese origin.

This post provides an overview of the vulnerability, analysis of Chaya_004 and mitigation recommendations, including proactive response measures taken by Forescout.

CVE-2025-31324: SAP Vulnerability Overview

CVE-2025-31324 allows attackers to achieve remote code execution (RCE) by uploading malicious web shells through a vulnerable endpoint in SAP NetWeaver Visual Composer. Attackers have demonstrated consistent exploitation patterns with:

- POST requests targeting the /developmentserver/metadatauploader endpoint.
- Deployment of web shells, including files named helper.jsp, cache.jsp, and others with randomized 8-letter names, such as "ssonkfrd.jsp".
- Use of curl to download further malicious payloads from external infrastructure.

Visual Composer is SAP's web-based tool to create business applications visually. It runs on NetWeaver servers that often serve other applications in the SAP business suite, such as customer relationship management (CRM), supply chain management (SCM) and supplier relationship management (SRM).

If left unpatched, exploitation of CVE-2025-31324 can lead to:

- **Service Disruption** – Web shell access may allow attackers to corrupt or delete Universal Description Discovery and Integration (UDDI) entries, disrupting communication between SAP modules like CRM, SCM, or SRM.
- **Information Leakage** – Service metadata can expose internal APIs, authentication methods, and system configurations.

- **Credential Interception** – Manipulated service endpoints may be used to harvest user credentials or inject malicious content.
- **Lateral Movement** – From Visual Composer, attackers can pivot toward more critical SAP components such as the Gateway, Message Server, or HANA database.
- **Regulatory Non-Compliance** – Unauthorized access or data manipulation may violate GDPR, HIPAA, SOX, and other data protection frameworks.

Exploitation: Opportunistic Scans and Hints of a Campaign

To identify current exploitation campaigns and actors, we have been using three data sources:

Scans on AEE. Several scanning tools and proof-of-concept (PoC) exploits have been released since April 25, a day after the CVE was published. We started noticing scans on the AEE since April 29, as shown in the figure below. Scans for "/developmentserver/metadatauploader" – looking for vulnerable servers – have been growing since April 29, while scans for "/irj/*.jsp" – looking for compromised servers – only happened between April 29 and April 30. We noticed 37 unique IP addresses scanning for "/developmentserver/metadatauploader" and 14 scanning for "/irj/*.jsp". All IPs related to the former scan were on Microsoft ASNs and all IPs related to the latter were on Amazon ASNs. No IP address was related to both scans. These IPs are reported in the IoC section of this blog, but they are likely related to benign scans given the ASNs and the fact that several carried the Zgrab user agent.

- **Exploitation attempts at customers.** Attempted exploitation has been observed primarily in manufacturing environments, where compromised SAP systems may lead to broad operational and security impacts. It's also important to notice that in these environments we observed reports of system crashes during defensive scans, indicating fragile or exposed installations. We observed 13 unique IP addresses attempting to exploit the vulnerability on customer networks. These addresses belong to the following ASes:
  - AS12876 (Scaleway S.A.S.) – French hosting provider with multiple IPs documented in brute force attacks targeting.
  - AS51167 (Contabo GmbH) – German hosting provider known for offering low-cost VPS services that are sometimes abused by threat actors.
  - AS40021 (Nubes, LLC) – US-based provider registered that hosts VPN servers and Tor services.
  - AS41314 (ECO TRADE Sp. z o.o.) – Small Polish ASN that seems to belong to a legitimate food manufacturing business. The IPs used in the exploitation attempts could have been compromised.
- **Tracking adversary infrastructure.** From one of the attacks, we recovered an ELF binary named "config" (888e953538ff668104f838120bc4d801c41adb07027db16281402a62f6ec29ef) and extracted from it IP address 47.97.42[.]177. That IP address hosted a SuperShell login interface at http://47.97.42[.]177:8888/supershell/login. SuperShell is a web-based reverse shell developed in Go by a Chinese-speaking developer called "tdragon6." This finding prompted us to map and track the threat actor infrastructure behind these exploits.

Mapping the Campaign: Uncovering the Chaya_004 Infrastructure

On the same IP address hosting Supershell (47.97.42[.]177), we also identified several other open ports, including 3232/HTTP using an anomalous self-signed certificate impersonating Cloudflare with the following properties: `Subject DN: C=US`, `O=Cloudflare, Inc`, `CN=:3232`.

Using Censys, we identified 114 IP addresses across 20 ASNs and 8 countries that shared the same uncommon CN on their certificates. Using FOFA, we saw 464 additional IP addresses across 17 ASNs and 19 countries with the same property. The ASNs with the most IP addresses were all based in China:

- ALIBABA-CN-NET (Hangzhou Alibaba Advertising Co.,Ltd.)
- TENCENT-NET-AP (Shenzhen Tencent Computer Systems Company Limited)
- HWCSNET (Huawei Cloud Service data center)
- CHINA169-BACKBONE (CHINA UNICOM China169 Backbone)

Other ASNs were mainly located in the US, Singapore and Japan with limited presence in several other countries.

787 of those IP addresses had port 3232 open, which matched the unusual CN value in the certificates and provided strong evidence of campaign consistency. Other commonly open ports included 443 (51 instances), 2096 (12 instances), 22 (9 instances), 3333 (6 instances) and 2222 (6 instances).

After mapping the infrastructure, we explored accessible web interfaces to identify deployed tools and found the following:

- NPS: Chinese-language GitHub repository for a "lightweight, high-performance, powerful intranet penetration proxy server"
- SuperShell: Primary backdoor/management interface
- SoftEther VPN: VPN client used for secure communications with compromised infrastructure on 45.94.43[.]41
- NHAS: Penetration testing toolkit
- Cobalt Strike: Commercial red team tool
- Asset Reconnaissance Lighthouse (ARL): Chinese-language GitHub repository for an asset discovery framework
- Pocassit: Chinese-language GitHub repository for a vulnerability scanning utility
- Gosint: Intelligence gathering framework
- GO Simple Tunnel: Chinese-language GitHub repository for a "simple tunnel written in Go"

The use of Chinese cloud providers and several Chinese-language tools points to a threat actor likely based in China, which we dubbed Chaya_004. Pivoting off the identified infrastructure led to additional findings related to Chaya_004:

- IP address 49.232.93[.]226, which historically distributed malware samples, including `svchosts.exe` (`f1e505fe96b8f83c84a20995e992b3794b1882df4954406e227bd7b75f13c779`). This sample has Triage watermark The same watermark was found in 28 IPs mainly in China, possibly connected to previously observed activity. This sample used domain http://search-email[.]com:443/ServiceLogin/_/kids/signup/eligible for C2 communication.
- An automated penetration testing tool hosted at http://8.210.65[.]56:5000/ with the following platform capabilities:
  - Asset reconnaissance modules (Hunter, Fofa, Quake, SecurityTrails, Subfinder)
  - Vulnerability scanning modules (Lighthouse, Xray proxy, AWVS)
  - Task orchestration and reporting capabilities

Mitigation Recommendations and Forescout Response

To defend against CVE-2025-31324:

1. **Apply SAP Patches Immediately** – SAP released fixes in the April 2025 Patch Day. Ensure you apply the appropriate security notes for NetWeaver AS Java versions 7.50–7.52.
2. **Restrict Access to Metadata Uploader Services** – Limit exposure of the /developmentserver/metadatauploader endpoints using firewall policies or SAP Web Dispatcher. Internal access should be restricted to authorized administrators.
3. **Disable Unused Web Services** – If the Visual Composer service is non-essential, consider disabling it entirely.
4. **Monitor for Anomalies** – Deploy real-time monitoring for abnormal access or changes to service entries, especially outside of maintenance windows.
5. **Conduct Regular Security Assessments** – Ensure SAP NetWeaver endpoints are included in routine penetration testing and vulnerability scans.

Beyond uncovering malicious infrastructure, Forescout's rapid threat research, detection engineering and collaboration with industry partners enabled a timely and effective response to CVE-2025-31324. As exploitation continues in the wild, we strongly urge all organizations running affected SAP versions to take immediate action.

Forescout rapidly deployed countermeasures across its product portfolio to help customers detect, respond to, and mitigate this threat:

- **OT/eyeInspect:** *Forescout's deep packet inspection and protocol analysis platform for OT and IoT networks.*
-
  - **Development of detection logic** for suspicious file uploads and malicious JSP web shell execution targeting SAP NetWeaver Visual Composer.
  - **Integration of threat intelligence and IoCs** from Vedere Labs, Onapsis, Red Canary, and Crowdsec to enrich detection capabilities.
  - **Continuous CVE DB enrichment**, enabling OT/eyeInspect to flag vulnerable SAP assets and correlate them with anomalous behaviors.
- **eyeFocus:** *Forescout's asset intelligence and vulnerability contextualization engine, providing global risk visibility across the enterprise.*
  - **Aggregation of threat intelligence and IoCs** related to CVE-2025-31324 from Vedere Labs and partner sources, improving risk scoring of affected systems.
  - **Integration of the CVE database**, enabling visibility into which SAP systems are exposed and prioritizing patching efforts based on business context.

- **eyeAlert:** *Forescout's real-time alerting and automation platform for security operations.*
  - **Implementation of eyeAlert rules** designed to detect CVE-2025-31324 exploitation attempts, such as anomalous POST requests to known vulnerable endpoints.
  - **Alert correlation with threat intelligence** to provide contextual alerts tied to observed attack behaviors (e.g., webshell activity, outbound curl connections).
  - **Flexible response actions** can be triggered, including segmentation, notifications, and integrations with SIEM/SOAR platforms.

This layered response across Forescout products ensures that both visibility and response capabilities are tightly aligned, giving customers a defense-in-depth approach to this vulnerability.

IoCs and Other Threat Intelligence Sources

The indicators of compromise (IoCs) below are available on the Forescout Vedere Labs threat feed.

IoC	Description
130.131.160[.]24 135.119.17[.]221 135.233.112[.]100 172.212.216[.]128 172.212.219[.]49 20.118.200[.]88 20.118.33[.]20 20.15.201[.]23 20.150.192[.]195 20.150.192[.]39 20.150.202[.]153 20.150.202[.]55 20.150.205[.]154 20.163.15[.]93 20.163.2[.]229 20.163.57[.]193 20.163.60[.]206 20.163.74[.]20 20.168.121[.]119 20.169.105[.]57 20.169.48[.]134 20.169.48[.]59 20.171.29[.]48 20.171.30[.]196 20.171.30[.]224 20.171.9[.]108 20.29.24[.]163 20.29.42[.]207 20.46.234[.]65 20.65.193[.]234 20.65.194[.]105 20.65.194[.]9 20.65.195[.]124 20.65.195[.]20 20.98.152[.]33 40.67.161[.]44 52.248.40[.]89	Observed scanning for /developmentserver/metadatauploader/ on AEE

13.228.100[.]218 13.58.39[.]15 18.142.70[.]42 18.159.188[.]112 18.204.33[.]8 3.12.99[.]176 3.19.125[.]50 3.229.147[.]107 3.65.236[.]123 3.65.237[.]228 3.77.117[.]203 34.193.126[.]209 35.157.196[.]116 52.74.236[.]95	Observed scanning for /irj/*.jsp on AEE
163.172.146[.]243 212.28.183[.]85 212.47.227[.]221 212.56.34[.]86 31.220.89[.]227 51.15.223[.]138 51.158.64[.]240 51.158.97[.]138 89.117.18[.]228 89.117.18[.]230 94.72.102[.]203 94.72.102[.]225 94.72.102[.]253	Observed attempting to exploit the vulnerability on customer networks
47.97.42[.]177 (Initial SuperShell host) 49.232.93[.]226 (malware distribution node) 8.210.65[.]56 (automated pentest platform) search-email[.]com (C2 domain) 888e953538ff668104f838120bc4d801c41adb07027db16281402a62f6ec29ef (config ELF binary) f1e505fe96b8f83c84a20995e992b3794b1882df4954406e227bd7b75f13c779 (svchosts.exe) Subject DN: C=US, O=Cloudflare, Inc, CN=:3232	Chaya_004 infrastructure

Other threat intelligence sources for CVE-2025-31324 include:

- **PoC exploit** released publicly: https://github.com/ODST-Forge/CVE-2025-31324_PoC
- **Exploitation analysis:** Rapid7 Blog on CVE-2025-31324
- **Detection rule (YARA):** Onapsis YARA Rule

Get all of Forescout's research from Vedere Labs in your inbox once a month.

Sign Up Now