مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Zero-Day Vulnerability in SAP NetWeaver

Tracking #:432317122

Date:25-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical unauthenticated remote code execution (RCE) vulnerability affecting SAP NetWeaver Visual Composer MetadataUploader has been identified and is now being actively exploited by threat actors in the wild.

TECHNICAL DETAILS:

A critical unauthenticated remote code execution (RCE) vulnerability affecting SAP NetWeaver Visual Composer MetadataUploader has been identified and is now being actively exploited by threat actors in the wild. Tracked as **CVE-2025-31324**, the vulnerability has been assigned a **CVSS v3.1 base score of 10.0**, indicating maximum severity.
Discovered by ReliaQuest Threat Research Team during recent incident response engagements, this zero-day flaw enables attackers to upload and execute malicious Java Server Pages (JSP) webshells—bypassing authentication and patch controls on even fully updated systems. Attackers are leveraging this flaw to gain **complete control over vulnerable SAP systems**, primarily targeting **enterprise and government networks**.

Vulnerability Details:

- CVE-2025-31324
- CVSS Score: 10.0 (Critical)
- SAP NetWeaver Visual Composer
- Component: Metadata Uploader
- Weakness: CWE-434 – Unrestricted Upload of File with Dangerous Type

IOCs:

1f72bd2643995fab4ecf7150b6367fa1b3fab17afd2abed30a98f075e4913087	Helper.jsp webshell
794cb0a92f51e1387a6b316b8b5ff83d33a51ecf9bf7cc8e88a619ecb64f1dcf	Cache.jsp webshell

RECOMMENDATIONS:

- Apply the latest patch provided by SAP immediately.
- Restrict access to the Metadata Uploader component until patches can be applied.
- Review external exposure of SAP components and ensure only authenticated users have upload permissions.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://reliaquest.com/blog/threat-spotlight-reliaquest-uncovers-vulnerability-behind-sap-netweaver-compromise/