

Forum:[Hack Forums](#)

Thread: [SAP fixes maximum severity NetWeaver command execution flaw - 21 vulns identified](#)

MadScientist - September 14, 2025, 9:57 pm

SAP has addressed 21 new vulnerabilities affecting its products, including three critical severity issues impacting the NetWeaver software solution.

SAP NetWeaver is the foundation for SAP's business apps like ERP, CRM, SRM, and SCM, and acts as a modular middleware that is broadly deployed in large enterprise networks.

In its security bulletin for September, the provider of enterprise resource planning (ERP) software lists a vulnerability with a maximum severity score of 10 out of 10 that is identified as CVE-2025-42944.

The security issue is an insecure deserialization vulnerability in SAP NetWeaver (RMIP4), ServerCore 7.50.

An unauthenticated attacker could exploit it to achieve arbitrary OS command execution by sending to an open port a malicious Java object through the RMI-P4 module.

RMI-P4 is the Remote Method Invocation protocol used by SAP NetWeaver AS Java for internal SAP-to-SAP communication, or for administration.

Though the P4 port is open on the host, some organizations may inadvertently expose it to wider networks, or the internet, due to firewall or other misconfigurations.

According to the security bulletin, the second critical flaw SAP fixed this month is CVE-2025-42922 (CVSS v3.1 score: 9.9), an insecure file operations bug impacting NetWeaver AS Java (Deploy Web Service), J2EE-APPS 7.50.

An attacker with non-administrative authenticated access can exploit a flaw in the web service deployment functionality to upload arbitrary files, potentially allowing full system compromise.

The third flaw is a missing authentication check in NetWeaver, tracked under CVE-2025-42958 (CVSS v3.1 score: 9.1).

This vulnerability allows unauthorized high-privileged users to read, modify, or delete sensitive data and access administrative functionality.

SAP also addressed the following new high-severity flaws:

CVE-2025-42933 (SAP Business One SLD): Insecure storage of sensitive data (e.g., credentials) that could be extracted and abused.

CVE-2025-42929 (SLT Replication Server): Missing input validation allowing malicious input to corrupt or manipulate replicated data.

CVE-2025-42916 (S/4HANA): Missing input validation in core components, risking unauthorized data manipulation.

SAP products, deployed by large organizations and often handling mission-critical data, are often

targeted by threat actors seeking high-value compromises.

Earlier this month, it was revealed that hackers were exploiting a critical code injection vulnerability tracked as CVE-2025-42957, impacting S/4HANA, Business One, and NetWeaver products.

System administrators are recommended to follow the patching and mitigation recommendations for the three critical flaws, available here (1, 2, 3) for customers with a SAP account.

Source -

<https://www.bleepingcomputer.com/news/security/sap-fixes-maximum-severity-netweaver-command-execution-flaw/>