NCA-44.091625 – National CERT Advisory – Critical Vulnerabilities in SAP NetWeaver

Introduction

Multiple critical vulnerabilities have been disclosed in SAP NetWeaver that allow unauthenticated remote code execution, insecure file operations, and unauthorized access. The most severe vulnerability (CVE-2025-42944, CVSS 10.0) impacts the RMI-P4 module and enables unauthenticated attackers to execute arbitrary operating system commands remotely. Other flaws (CVE-2025-42922, CVSS 9.9 and CVE-2025-42958, CVSS 9.1) may permit insecure file uploads and bypass of authentication mechanisms, leading to privilege escalation and data compromise.

Given SAP NetWeaver's widespread usage in enterprise environments, these vulnerabilities pose a severe risk of system compromise, malware deployment, and unauthorized access to sensitive information.

Impact

Successful exploitation can lead to:

1. **Unauthorized Code Execution** – Remote command execution via deserialization vulnerability.
2. **System Compromise** – Full takeover of affected SAP NetWeaver servers.
3. **Malware Deployment** – Upload and execution of arbitrary files.
4. **Unauthorized Privileged Access** – Authentication bypass allowing attackers to gain higher-level access.
5. **Data Exposure** – Theft or tampering of sensitive enterprise data.

Threat Details

Vulnerability Overview

- **Incident ID:** Critical Vulnerabilities – SAP NetWeaver
- **Affected Components:**
    - SAP NetWeaver ServerCore 7.50 (RMI-P4 module) – CVE-2025-42944
    - SAP NetWeaver J2EE-APPS 7.50 (Deploy Web Service module) – CVE-2025-42922
    - SAP NetWeaver Authentication Flaw (General NetWeaver platforms) – CVE-2025-42958

- **Description:** Remote code execution, insecure file operations, and authentication bypass vulnerabilities in SAP NetWeaver.

Attack Complexity & Vector

- **Attack Vector:** Remote (network accessible modules)
- **Attack Complexity:** Low (exploitation straightforward with crafted requests)
- **Privileges Required:** None (CVE-2025-42944 exploitable unauthenticated)
- **User Interaction:** None required
- **Estimated CVSS v3.1 Score:**
    - CVE-2025-42944 – 10.0 (CRITICAL)
    - CVE-2025-42922 – 9.9 (CRITICAL)
    - CVE-2025-42958 – 9.1 (CRITICAL)
- **Relevant CWEs:**
    - CWE-502: Deserialization of Untrusted Data
    - CWE-434: Unrestricted File Upload
    - CWE-287: Improper Authentication

Exploit Conditions

Exploitation requires:

- Network access to exposed RMI-P4 or Deploy Web Service modules.
- No authentication in the case of CVE-2025-42944.
- Use of default/weak configurations allowing arbitrary file upload or missing authentication checks.

Recommendations & Mitigation Actions

1. Patch Immediately (Recommended Fix)

- Apply SAP-released patches (as of September 9, 2025) for Notes 3643501, 3643865, and 3642961.
- Update all affected NetWeaver instances to the fixed versions.

2. Temporary Mitigation (If Patching Not Possible)

- Restrict network access to the RMI-P4 module (e.g., block/filter traffic at the ICM or firewall).
- Restrict Deploy Web Service access to only trusted/necessary accounts.
- Validate and restrict uploaded file types; disable or limit “deploy” / “upload” functionality if not required.

3. Strengthen Security Posture

- Conduct configuration reviews to ensure only required modules are exposed.
- Implement strict network segmentation around SAP NetWeaver servers.
- Enable logging and continuous monitoring for anomalous activity (unexpected file uploads, OS command execution, or privilege escalation attempts).

Monitoring & Detection

- Monitor for abnormal execution of system commands from NetWeaver processes.
- Track file uploads to ensure only authorized sources are permitted.
- Review authentication logs for suspicious or bypassed login attempts.
- Use IDS/IPS and SIEM solutions to detect traffic anomalies to/from RMI-P4 and Deploy Web Service modules.

Incident Response & Readiness

- Ensure incident response teams are briefed on these vulnerabilities.
- Validate backups and recovery procedures for NetWeaver systems.
- Review SAP application logs for exploitation attempts and uploaded malicious files.
- Rotate credentials for accounts with elevated privileges if compromise is suspected.

Patching Summary

Version Category	SAP NetWeaver Components	Status
Vulnerable	ServerCore 7.50 (RMI-P4), J2EE-APPS 7.50 (Deploy Web Service), General NetWeaver Authentication	Must patch immediately
Secure	Patched versions with SAP Notes 3643501, 3643865, 3642961	No action required

References

- SAP – Security Patch Notes (#3643501, #3643865, #3642961)
- Onapsis – SAP Security Notes September 2025 Patch Day
- PurpleOps – SAP Security Patch Day Addresses 21 Vulnerabilities, 4 Classified as Critical: CVE-2025-42944 (CVSS 10.0)

Call to Action

The National CERT advises all organizations using SAP NetWeaver to:

- Immediately apply the released patches.
- Restrict access to vulnerable modules until patching is complete.

- Monitor systems closely for exploitation attempts.
- Review access logs and uploaded files for signs of compromise.

Timely remediation is critical to prevent remote code execution, malware deployment, and full system compromise.