Security Advisory 2026-011

Critical Vulnerabilities in SAP Kernel and NetWeaver Message Server

2026-09-09 — v1.0

TLP:CLEAR

History:

- 09/09/2026 — v1.0 – Initial publication.

Summary

On 8 September 2026, as part of its September Security Patch Day, SAP released Security Notes addressing two critical vulnerabilities affecting a broad range of SAP products [1][3]. The most severe, CVE-2026-44756 (CVSS 10.0), is a memory corruption vulnerability in SAP Extended Passport (EPP) processing, nicknamed "OVERPASS" by the Onapsis Research Labs (ORL), which discovered and responsibly disclosed it [2][3]. The second, CVE-2026-58240 (CVSS 9.8), nicknamed "S4GET", is a missing authentication check in the SAP NetWeaver Message Server [3][6].

Both are remotely exploitable without authentication. According to the reporting researchers, successful exploitation of either can result in arbitrary operating system command execution under the account that owns the SAP installation, leading to full compromise of the affected system and the business data it holds [2][6].

CERT-EU strongly recommends applying SAP Security Notes 3747649 and 3759472 as soon as possible [1].

Technical Details

CVE-2026-44756 - "OVERPASS" (CVSS 10.0)

CVE-2026-44756 is a memory corruption vulnerability in the SAP Kernel library that processes the Extended Passport (EPP), addressed by SAP Security Note 3747649 [1][4]. SAP's CVE record states that boundary validation is missing during the deserialisation of EPP data, and that an unauthenticated attacker can send a crafted network request containing a malformed EPP header, potentially resulting in undefined behaviour and abnormal program termination, with a high impact on confidentiality, integrity, and availability [2][3].

Onapsis, which reported the vulnerability, assesses that successful exploitation allows a remote attacker to execute arbitrary operating system commands on the SAP host with SAP administrative privileges, resulting in full compromise of the underlying SAP business data and processes [2].

CVE-2026-58240 - "S4GET" (CVSS 9.8)

CVE-2026-58240 is a missing authentication check in the SAP NetWeaver Message Server (component BC-CST-MS), addressed by SAP Security Note 3759472 [1][5]. The Message Server does not sufficiently validate the authenticity of internal application server components during registration. Consequently, an unauthenticated attacker with network access can register unauthorised components and potentially perform unauthorised actions within the application environment, resulting in a high impact on the confidentiality, integrity, and availability of the affected system [3][5].

Onapsis, which also reported this vulnerability, states that an attacker can promote themselves to a trusted node inside an SAP cluster, that the Message Server propagates that trust to every application server in the cluster, and that a successful attack yields remote code execution as the operating-system user that runs SAP [6]. Onapsis notes the flaw is reachable through the same public port that SAP GUI clients connect to, which cannot be firewalled without breaking end-user logon [6].

Affected Products

CVE-2026-44756 – affected versions [1]:

- KRNL64NUC 7.22, 7.22EXT
- KRNL64UC 7.22, 7.22EXT, 7.53, 8.04
- KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 8.04, 9.16, 9.18, 9.19, 9.20
- WEBDISP 9.16, 9.18, 9.19, 9.20

CVE-2026-58240 – affected versions [1]:

- KERNEL 9.16, 9.18, 9.19, 9.20

Recommendations

CERT-EU strongly recommends following **SAP Security Note 3747649** (CVE-2026-44756) and **SAP Security Note 3759472** (CVE-2026-58240) to update the affected products to the relevant versions as soon as possible [1].

References

[1] https://support.sap.com/en/my-support/knowledge-base/security-notes-news/september-2026.html

[2] https://onapsis.com/blog/sap-overpass-remediation/

[3] https://onapsis.com/blog/sap-security-patch-day-september-2026/

[4] https://www.cve.org/CVERecord?id=CVE-2026-44756

[5] https://www.cve.org/CVERecord?id=CVE-2026-58240

[6] https://onapsis.com/blog/s4get-cve-2026-58240-sap-message-server-threat-advisory/