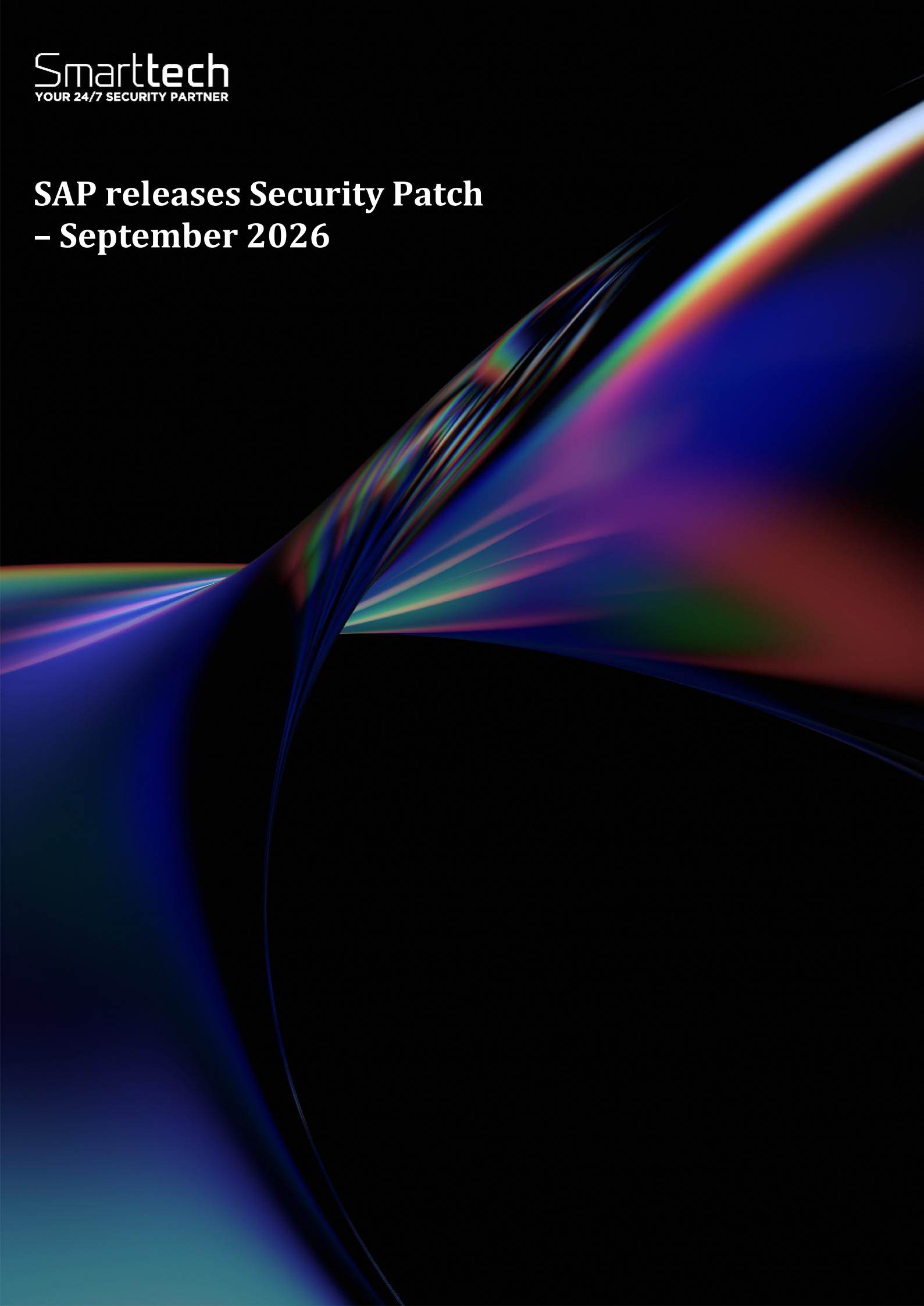
Smarttech
YOUR 24/7 SECURITY PARTNER

# SAP releases Security Patch – September 2026



| | |
|---|---|
| **Document ID** | SMA-Threat Report |
| **Document status** | ISSUED |
| **Issue Number** | 156 |
| **Authors** | Gabriel Gheorghiu < gabriel.gheorghiu@smarttech247.com > |
| **Verified by** | Alin Curcan < alin.curcan@smarttech247.com > |
| **Last modified** | 2026-09-09 |
| **Issue Date** | 2026-09-09 |

**Threat Reports** are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

## Overview:

SAP released set of security updates, addressing multiple vulnerabilities across SAP products, including SAP NetWeaver, SAP Kernel, SAP CAP, and SAP S/4HANA. The release contains several Critical and High-severity vulnerabilities. The vulnerabilities include memory corruption, missing authentication and authorization checks, credential disclosure, privilege escalation, and injection flaws. Successful exploitation could lead to remote code execution, unauthorized access, data exposure, privilege escalation, and disruption of business-critical SAP services.

### Risk

Government:

- Large and medium government entities: Critical
- Small government entities: High

Businesses:

- Large and medium business entities: Critical
- Small business entities: High

## Technical summary

More details related to the Critical and High-severity vulnerabilities are as follows:

| ***CVE ID*** | ***Description*** |
|---|---|
| **CVE-2026-44756**<br>**CVSS Score: 10**<br>**Memory Corruption vulnerability in SAP Extended Passport (EPP) Processing** | A memory corruption vulnerability that could allow an unauthenticated attacker to execute arbitrary code and compromise the confidentiality, integrity, and availability of affected systems. |
| **CVE-2026-58240**<br>**CVSS Score: 9.8**<br>**Missing Authentication check in SAP NetWeaver (Message Server)** | Insufficient authentication controls may allow remote attackers to access services without proper authentication, potentially leading to unauthorized system access. |
| **CVE-2026-76969**<br>**CVSS Score: 9.4**<br>**Credential disclosure in multitenant applications using SAP Cloud Application Programming Model (CAP)** | A vulnerability that could expose sensitive credentials used by multitenant applications, potentially enabling unauthorized access to SAP resources. |

| | |
|---|---|
| **CVE-2026-66768**<br>**CVSS Score: 9.0**<br>**Improper Access Control in SAP NetWeaver (SAP GUI for Java)** | Improper access restrictions may allow attackers to gain access to functionality or data beyond their intended permissions. |
| **CVE-2026-58243**<br>**CVSS Score: 8.8**<br>**Privilege Escalation vulnerability in SAP ABAP Developer Tools** | An authenticated attacker could obtain elevated privileges, enabling unauthorized actions within the SAP environment. |
| **CVE-2026-76958**<br>**CVSS Score: 8.5**<br>**XML External Entity (XXE) Vulnerability in SAP Integration Suite** | Improper XML processing may allow attackers to access sensitive files, disclose information, or interact with internal resources. |
| **CVE-2026-76967**<br>**CVSS Score: 7.8**<br>**Insecure Deserialization in SAP NetWeaver Business Client** | Deserialization of untrusted data may allow execution of malicious code or manipulation of application behavior. |
| **CVE-2026-66767**<br>**CVSS Score: 7.7**<br>**Memory Corruption vulnerability in SAP NetWeaver Application Server for ABAP and ABAP** | A memory handling flaw that could result in application crashes or potential code execution under specific conditions. |
| **CVE-2026-2332**<br>**CVSS Score: 7.4**<br>**CLRF Injection vulnerability due to use of Jetty components in SAP Commerce Cloud (Search And Navigation)** | Improper input sanitization may allow attackers to manipulate HTTP responses, potentially leading to header injection or other attacks. |
| **CVE-2026-76968**<br>**CVSS Score: 6.5**<br>**Information Disclosure vulnerability in SAP Web Dispatcher, Internet Communication Manager and SAP Content Server** | Sensitive information may be exposed to unauthorized users, increasing the risk of reconnaissance and further compromise. |
| **CVE-2026-44766**<br>**CVSS Score: 6.5**<br>**SQL Injection vulnerability in SAP S/4HANA (Intercompany Matching and Reconciliation)** | Insufficient input validation may allow attackers to manipulate database queries and access or modify sensitive data. |
| **CVE-2026-76971**<br>**CVSS Score: 6.5**<br>**Server-Side Request Forgery in SAP Manufacturing Integration and Intelligence** | Attackers may be able to force the application to send requests to internal or external systems, potentially exposing internal resources. |

In addition to the Critical and High-severity vulnerabilities, SAP addressed multiple Medium-severity issues affecting SAP Commerce Cloud, SAPUI5, SAP S/4HANA, SAP NetWeaver, and SAP Process Integration. These vulnerabilities include authorization control weaknesses, cross-site request forgery (CSRF), clickjacking, security misconfigurations, and denial-of-service conditions, which could contribute to

unauthorized actions, reduced system availability, or facilitate further compromise when combined with other attack techniques.

## Recommendations

**Smarttech247** team recommend the following actions to be taken:

- Upgrade to the latest versions in order to obtain a fix for these vulnerabilities.
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner for prevention.
- Use the right Vulnerability Management Tools to assess endpoints, networks, or applications for known weaknesses.
- Apply the Principle of Least Privilege to all systems and services.
- Apply advanced application control and protection to enforce granular control over all application access, communications, and privilege elevation attempts.
- Ensure that your Endpoint Security and Perimeter security products are updated with the latest signatures to detect these threats.

## References

https://support.sap.com/en/my-support/knowledge-base/security-notes-news/september-2026.html?isu_page=1

### CVEs

CVE-2026-44756
CVE-2026-58240
CVE-2026-76969
CVE-2026-66768
CVE-2026-58243
CVE-2026-76958
CVE-2026-76967
CVE-2026-66767
CVE-2026-2332
CVE-2026-76968
CVE-2026-44766
CVE-2026-76971
CVE-2026-34477
CVE-2026-76977
CVE-2026-76960
CVE-2026-76961
CVE-2026-76959
CVE-2026-76962
CVE-2026-76963
CVE-2026-58234

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com