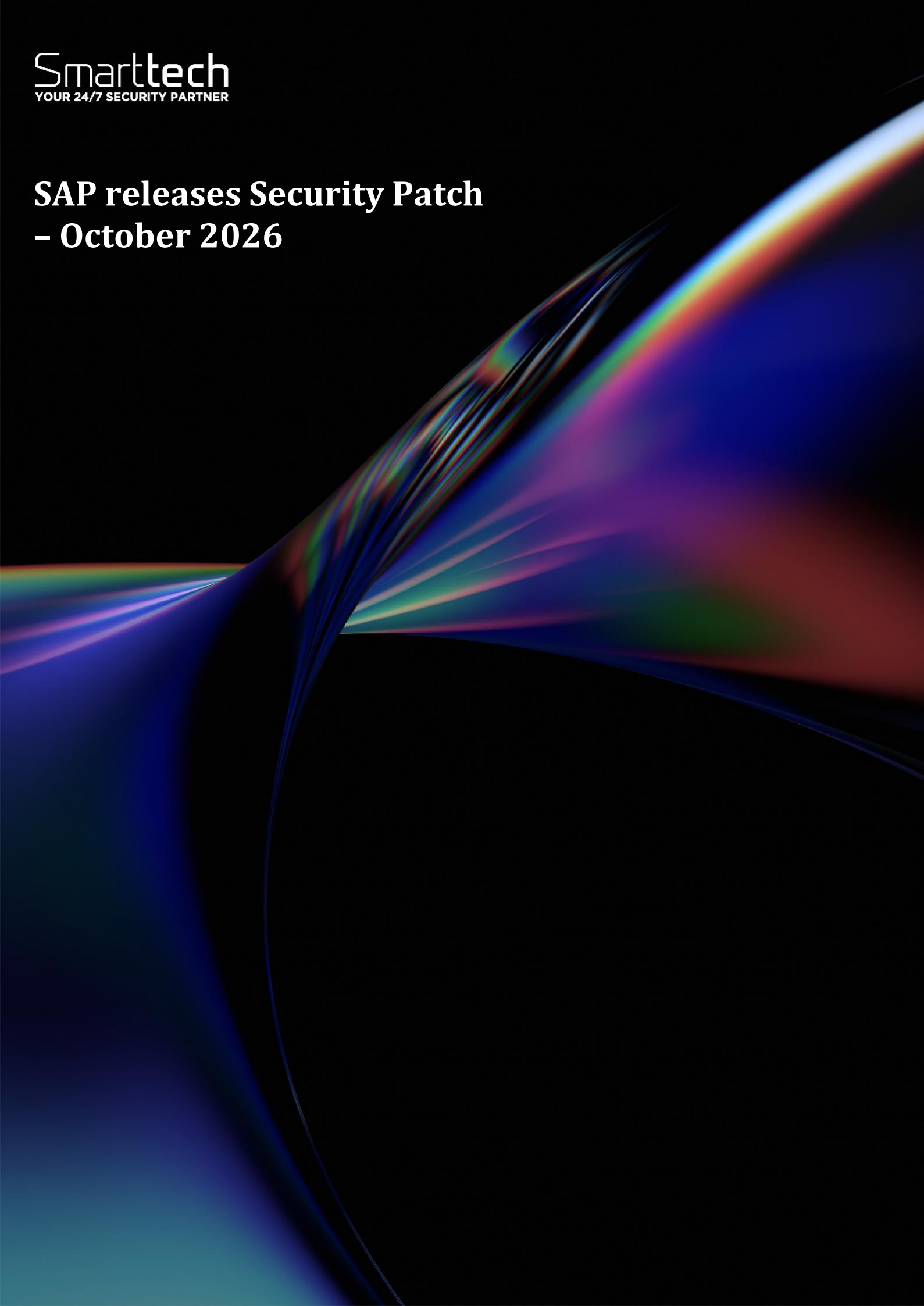


SAP releases Security Patch – October 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	170
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-10-13
Issue Date	2026-10-13

This document and any information therein are confidential property of Smarttech247 and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of Smarttech247, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Smarttech247 retain the right to alter the document at any time unless a written statement to the contrary has been appended.

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 a comprehensive set of security updates, several of these vulnerabilities are rated Critical (CVSS up to 10) or High, addressing severe issues such as server-side request forgery (SSRF), broken access control, missing authorization checks, code injection, SQL injection, memory corruption, command injection, improper authentication, information disclosure, and XSS. If exploited, these vulnerabilities could lead to remote code execution, unauthorized access, sensitive data exposure, and system compromise.

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 these vulnerabilities are as follows:

<u>CVE ID</u>	<u>Description</u>
CVE-2026-89111 CVSS Score: 10 OAuth2 SSRF vulnerability in SAP Cloud SDK for Python	The SAP Cloud SDK for Python contains an OAuth2 SSRF vulnerability affecting multi-tenant BTP applications. An attacker who controls the tenant_subdomain parameter can redirect OAuth2 token requests to an attacker-controlled server, causing client credentials to be exfiltrated.
CVE-2026-89110 CVSS Score: 9.9 Broken Access Control in SAP NetWeaver Visual Composer	SAP NetWeaver Visual Composer does not perform sufficient authorization checks in certain portal functionality. An attacker with low privileges could invoke internal operations on a preconfigured remote system. Depending on the remote connection configuration, this could lead to a full compromise of the remote system. This results in a high impact on confidentiality, integrity and availability.
CVE-2026-89107 CVSS Score: 9.9 Code Injection vulnerability in SAP S/4HANA (Manage Substitution/Validation Rules)	SAP S/4HANA (Manage Substitution/Validation Rules) does not sufficiently validate input processed by rule definition functionality that utilizes a domain-specific scripting language. An authenticated attacker with specific business privileges could submit specially crafted input, which is interpreted as executable ABAP code by the rule processing logic. Successful

	exploitation could allow the attacker to execute ABAP arbitrary code into the system, resulting in full compromise of the affected system and high impact on confidentiality, integrity, and availability of the system
CVE-2026-89108 CVSS Score: 9.1 Missing Authorization check in SAP Manufacturing Integration and Intelligence (Configuration Service)	SAP Manufacturing Integration and Intelligence does not sufficiently enforce authorization boundaries within certain administrative functionality. An attacker with MII administrator privileges could submit a specially crafted request to provision an account with elevated privileges on the underlying Java application server. Successful exploitation could allow the attacker to gain administrative control over the underlying system, extending the impact beyond the vulnerable application. This results in a high impact on confidentiality, integrity and availability.
CVE-2026-89113 CVSS Score: 8.8 SQL Injection vulnerability in SAP Commerce Cloud (OOTB Code)	SAP Commerce Cloud does not sufficiently validate certain user-supplied input before it is incorporated into a database query. An authenticated user could send specially crafted requests to affected functionality to inject arbitrary SQL commands. Successful exploitation could allow the user to read, modify or delete sensitive data from the application's database, resulting in a high impact on confidentiality, integrity and availability of the application.
CVE-2026-58249 CVSS Score: 7.5 Memory Corruption vulnerability in SAP NetWeaver and SAP Web Dispatcher (Internet Communication Manager)	SAP NetWeaver and SAP Web Dispatcher do not properly validate certain fields in specially crafted requests handled by an internal protocol component. An unauthenticated attacker could send a malicious request that triggers a memory-handling error, causing the affected process to crash. Successful exploitation can therefore result in a high impact on the availability of the affected application. There is no impact on the confidentiality or integrity of the application.
CVE-2026-89120 CVSS Score: 7.1 Missing authorization check in SAP ABAP Platform	A regression caused by an API change in SAP ABAP Platform reintroduces a previously fixed authorization weakness. The session manager can be opened in single transaction mode, including from FLP. A low-privileged attacker could exploit this to bypass restrictions via specially crafted requests, resulting in high impact on integrity and low impact on confidentiality. There is no impact on availability.
CVE-2026-89112 CVSS Score: 6.5 Broken Access Control in CLA-Assistant — CLA Signature PII Disclosure	The admin API endpoint used to retrieve CLA signature records does not consistently enforce the required authorization checks when the target organisation is specified using an organisation ID. An authenticated user with limited privileges could potentially access CLA signature records containing contributor information belonging to an organisation they are not authorized to administer.
CVE-2026-76972 CVSS Score: 6.5 Cross-Site Scripting (XSS) vulnerability in SAP Manufacturing Integration and Intelligence	Due to a Cross-Site Scripting (XSS) vulnerability in SAP Manufacturing Integration and Intelligence, an attacker could store malicious content that is later rendered by the application. If an authenticated victim accesses a page that displays this stored content, the injected input is processed during web page generation, resulting in the execution of malicious content in the victim's browser context. This could allow the attacker to access or modify information within the victim's browser scope. Successful exploitation could allow the attacker to access session information, modify rendered page content and disrupt the victim's use of the application, resulting in a low impact on confidentiality, integrity and availability.

CVE-2026-24316 CVSS Score: 6.4 Server-Side Request Forgery (SSRF) in SAP NetWeaver Application Server for ABAP	SAP NetWeaver Application Server for ABAP provides an ABAP Report for testing purposes, which allows to send HTTP requests to arbitrary internal or external endpoints. The report is therefore vulnerable to Server-Side Request Forgery (SSRF). Successful exploitation could lead to interaction with potentially sensitive internal endpoints, resulting in a low impact on data confidentiality and integrity. There is no impact on availability of the application.
CVE-2025-42938 CVSS Score: 6.1 Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver ABAP Platform	Due to a Cross-Site Scripting (XSS) vulnerability in the SAP NetWeaver ABAP Platform, an unauthenticated attacker could generate a malicious link and make it publicly accessible. If an authenticated user clicks on this link, the injected input is processed during the websites page generation, resulting in the creation of malicious content. When executed, this content allows the attacker to access or modify information within the victim's browser scope, impacting the confidentiality and integrity while availability remains unaffected.
CVE-2026-89117 CVSS Score: 6.1 Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Enterprise Portal	SAP NetWeaver Enterprise Portal allows an unauthenticated attacker to inject malicious scripts into a URL parameter. The scripts are reflected in the server response and executed in a user's browser when the crafted URL is visited, leading to theft of session information, manipulation of portal content, or user redirection. This results in a low impact on confidentiality and integrity. There is no impact on availability.
CVE-2026-76975 CVSS Score: 6.1 Cross-Site Scripting (XSS) vulnerability in SAPUI5 (Support Assistant Overlay)	Due to a DOM-Based Cross-Site Scripting (XSS) vulnerability, an unauthenticated attacker could generate a malicious link and make it publicly accessible. If an authenticated user accesses this link, client-side code reads the attacker-controlled input and writes it into the DOM without proper sanitization, causing attacker-supplied script to execute in the victim's browser context. This could allow the attacker to access or modify information within the victim's browser scope, impacting confidentiality and integrity, while availability remains unaffected.
CVE-2026-89122 CVSS Score: 6.1 Open Redirect Vulnerability in SAP NetWeaver Enterprise Portal	SAP NetWeaver Enterprise Portal does not sufficiently validate input to a certain portal component. An unauthenticated attacker could craft a malicious link that, when clicked by a victim, loads attacker-controlled content within the trusted application context. Successful exploitation could allow the attacker to track user information and deface parts of the rendered page, resulting in a low impact on confidentiality and integrity with no impact on availability.
CVE-2026-89116 CVSS Score: 5.9 OS Command Injection in Yeoman-UI / Application Wizard Extension for VS Code	The affected code used <code>child_process.execSync</code> with a shell string for generator installation and uninstallation. This allowed an attacker to execute arbitrary OS commands with the developer's privileges by manipulating the <code>ApplicationWizard.installationLocation</code> VS Code workspace configuration value. Because the value was passed directly to the shell without sanitisation, a malicious workspace repository could craft a <code>settings.json</code> that injects OS commands when a developer opens the project and triggers a generator installation.
CVE-2026-76976 CVSS Score: 5.4 Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Application Server	Applications based on SAP GUI for HTML in SAP NetWeaver Application Server ABAP do not sufficiently sanitize user-supplied content in certain functionality, allowing an authenticated attacker to send malicious content to another user. If the victim interacts with the affected content, malicious

ABAP (Applications based on SAP GUI for HTML)	scripts could be executed in the victim's browser context. This vulnerability has a low impact on the confidentiality and integrity of the data and no impact on the availability of the application.
CVE-2026-89118 CVSS Score: 5.3 Information Disclosure vulnerability in SAP NetWeaver Enterprise Portal	SAP NetWeaver Enterprise Portal allows an unauthenticated attacker to access restricted resources and retrieve non-critical application information, which leads to Low impact on Confidentiality, but there is no impact on Integrity and Availability of the application.
CVE-2026-89121 CVSS Score: 4.7 Missing Authorization Check in SAP S/4HANA (Linear Asset Management RAP Business Object)	SAP S/4HANA does not perform sufficient instance-level authorization checks for certain modification operations on associated business object data. An attacker with low privileges and local access to the system could bypass authorization checks to modify data belonging to objects they are not authorized for. This results in a high impact on integrity. There is no impact on confidentiality and availability.
CVE-2026-89106 CVSS Score: 4.4 Cross Site Scripting (XSS) vulnerability in SAPUI5	SAP UI5 does not perform sufficient input validation under certain configurations. An attacker with low privileges could submit specially crafted content that is later rendered in a victim's browser. This vulnerability has a low impact on confidentiality and integrity. There is no impact on availability.
CVE-2026-89124 CVSS Score: 4.3 Missing Authorization Check in SAP Global Trade Services, edition for SAP HANA (Display Product Catalog Based on Customs Declaration)	Display Product Catalog Based on Customs Declaration application does not perform sufficient authorization checks within certain functionality, allowing an authenticated low-privileged user to access sensitive information beyond their intended authorization scope. This vulnerability has low impact on confidentiality of the data, with no impact on the integrity and availability of the application.
CVE-2026-89105 CVSS Score: 4.2 Improper Authentication in HybridTokenAuthenticator of SAP/cloud-security-services-integration-library	The HybridTokenAuthenticator component of the SAP/cloud-security-services-integration-library accepts tokens from unintended ambient IAS/XSUAA bindings, potentially allowing unauthorized access. This vulnerability allows an attacker to gain unauthorized access to the system by using tokens that should not be accepted, leading to a breach of security.
CVE-2026-58242 CVSS Score: 3.5 Improper Authorization check in SAP Cloud Connector	SAP Cloud Connector contains an improper authorization check, which could be exploited by a low-privileged attacker through specially crafted requests. Exploitation requires the attacker to be on an adjacent network. Successful exploitation could allow the attacker to obtain limited information about internal systems, resulting in low impact on confidentiality. There is no impact on integrity and availability.

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/october-2026.html?isu_page=1

CVEs

CVE-2026-89111
CVE-2026-89110
CVE-2026-89107
CVE-2026-89108
CVE-2026-89113
CVE-2026-58249
CVE-2026-89120
CVE-2026-89112
CVE-2026-76972
CVE-2026-24316
CVE-2025-42938
CVE-2026-89117
CVE-2026-76975
CVE-2026-89122
CVE-2026-89116
CVE-2026-76976
CVE-2026-89118
CVE-2026-89121
CVE-2026-89106
CVE-2026-89124
CVE-2026-89105
CVE-2026-58242

