Smarttech
YOUR 24/7 SECURITY PARTNER

SAP releases Security Patch – February 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	21
Authors	Paula Radoi <paula.radoi@smarttech247.com>
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-02-11
Issue Date	2026-02-10

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, including 26 new Security Notes. Several of these vulnerabilities are rated Critical (CVSS up to 9.9) or High, with potential impacts such as unauthorized access, data tempering, authorization bypass, account impersonation and remote code execution.

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:

CVE ID	***Description***
CVE-2026-0488 - Code Injection vulnerability in SAP CRM and SAP S/4HANA (Scripting Editor) **CVSS Score: 9.9**	An authenticated attacker in SAP CRM and SAP S/4HANA (Scripting Editor) could exploit a flaw in a generic function module call and execute unauthorized critical functionalities, which includes the ability to execute an arbitrary SQL statement. This leads to a full database compromise with high impact on confidentiality, integrity, and availability.
CVE-2026-0509 - Missing Authorization check in SAP NetWeaver Application Server ABAP and ABAP Platform **CVSS Score: 9.6**	SAP NetWeaver Application Server ABAP and ABAP Platform allows an authenticated, low-privileged user to perform background Remote Function Calls without the required S_RFC authorization in certain cases. This can result in a high impact on integrity and availability, and no impact on the confidentiality of the application.
CVE-2026-23687 - XML Signature Wrapping in SAP NetWeaver AS ABAP and ABAP Platform **CVSS Score: 8.8**	SAP NetWeaver Application Server ABAP and ABAP Platform allows an authenticated attacker with normal privileges to obtain a valid signed message and send modified signed XML documents to the verifier. This may result in acceptance of tampered identity information,

	unauthorized access to sensitive user data and potential disruption of normal system usage.
CVE-2026-23689 - **Denial of service (DOS) in SAP Supply Chain Management** **CVSS Score: 7.7**	Due to an uncontrolled resource consumption (Denial of Service) vulnerability, an authenticated attacker with regular user privileges and network access can repeatedly invoke a remote-enabled function module with an excessively large loop-control parameter. This triggers prolonged loop execution that consumes excessive system resources, potentially rendering the system unavailable. Successful exploitation results in a denial-of-service condition that impacts availability, while confidentiality and integrity remain unaffected.
CVE-2026-0492 - **Missing Authorization check in SAP Solution Tools Plug-In (ST-PI)** **CVSS Score: 7.7**	SAP Solution Tools Plug-In (ST-PI) contains a function module that does not perform the necessary authorization checks for authenticated users, allowing sensitive information to be disclosed. This vulnerability has a high impact on confidentiality and does not affect integrity or availability.
CVE-2026-0490 - **Denial of service (DOS) in SAP BusinessObjects BI Platform** **CVSS Score: 7.5**	SAP BusinessObjects BI Platform allows an unauthenticated attacker to craft a specific network request to the trusted endpoint that breaks the authentication, which prevents the legitimate users from accessing the platform. As a result, it has a high impact on the availability but no impact on the confidentiality and integrity.
CVE-2026-0485 - **Denial of service (DOS) vulnerability in SAP BusinessObjects BI Platform** **CVSS Score: 7.5**	SAP BusinessObjects BI Platform allows an unauthenticated attacker to send specially crafted requests that could cause the Content Management Server (CMS) to crash and automatically restart. By repeatedly submitting these requests, the attacker could induce a persistent service disruption, rendering the CMS completely unavailable. Successful exploitation results in a high impact on availability, while confidentiality and integrity remain unaffected.
CVE-2025-12383 - **Race Condition in SAP Commerce Cloud** **CVSS Score: 7.4**	In Eclipse Jersey versions 2.45, 3.0.16, 3.1.9 a race condition can cause ignoring of critical SSL configurations - such as mutual authentication, custom key/trust stores, and other security settings. This issue may result in SSLHandshakeException under normal circumstances, but under certain conditions, it could lead to unauthorized trust in insecure servers (see PoC)
CVE-2026-0508 - **Open Redirect vulnerability in SAP BusinessObjects Business Intelligence Platform** **CVSS Score: 7.3**	The SAP BusinessObjects Business Intelligence Platform allows an authenticated attacker with high privileges to insert malicious URL within the application. Upon successful exploitation, the victim may click on this malicious URL, resulting in an unvalidated redirect to the attacker-controlled domain and subsequently download the malicious content. This vulnerability has a high impact on the confidentiality and integrity of the application, with no effect on the availability of the application.
CVE-2026-0484 - **Missing Authorization check in SAP NetWeaver Application Server ABAP and SAP S/4HANA** **CVSS Score: 6.5**	Due to missing authorization check in SAP NetWeaver Application Server ABAP and SAP S/4HANA, an authenticated attacker could access a specific transaction code and modify the text data in the system. This vulnerability has a high impact on integrity of the

	application with no effect on the confidentiality and availability.
CVE-2026-24324 - Denial of service (DOS) vulnerability in SAP BusinessObjects Business Intelligence Platform (AdminTools) **CVSS Score: 6.5**	SAP BusinessObjects Business Intelligence Platform (AdminTools) allows an authenticated attacker with user privileges to execute a specific query in AdminTools that could cause the Content Management Server (CMS) to crash, rendering the CMS partially or completely unavailable and resulting in the denial of service of the Content Management Server (CMS). Successful exploitation impacts system availability, while confidentiality and integrity remain unaffected.
CVE-2026-0505, CVE-2026-24323 - Multiple vulnerabilities in BSP Applications of SAP Document Management System **CVSS Score: 6.1**	The BSP applications allow an unauthenticated user to inject malicious script content via user-controlled URL parameters that are not sufficiently sanitized. When a victim accesses a crafted URL, the injected script is executed in the victim□s browser, leading to a low impact on confidentiality and integrity, and no impact on the availability of the application. The BSP applications allow an unauthenticated user to manipulate user-controlled URL parameters that are not sufficiently validated. This could result in unvalidated redirection to attacker-controlled websites, leading to a low impact on confidentiality and integrity, and no impact on the availability of the application.
CVE-2026-24328 - Open Redirection vulnerability in Business Server Pages Application (TAF_APPLAUNCHER) **CVSS Score: 6.1**	SAP TAF_APPLAUNCHER within Business Server Pages allows unauthenticated attacker to craft malicious links that, when clicked by a victim, redirect them to attacker?controlled sites, potentially exposing or altering sensitive information in the victim□s browser. This results in a low impact on confidentiality and integrity, with no impact on the availability of the application.
CVE-2025-0059 - Information Disclosure vulnerability in SAP NetWeaver Application Server ABAP (applications based on SAP GUI for HTML) **CVSS Score: 6.0**	Applications based on SAP GUI for HTML in SAP NetWeaver Application Server ABAP store user input in the local browser storage to improve usability. An attacker with administrative privileges or access to the victim□s user directory on the Operating System level would be able to read this data. Depending on the user input provided in transactions, the disclosed data could range from non-critical data to highly sensitive data, causing high impact on confidentiality of the application.
CVE-2026-23684 - Race condition vulnerability in SAP Commerce Cloud **CVSS Score: 5.9**	A race condition vulnerability exists in the SAP Commerce cloud. Because of this when an attacker adds products to a cart, it may result in a cart entry being created with erroneous product value which could be checked out. This leads to high impact on data integrity, with no impact on data confidentiality or availability of the application.
CVE-2026-24319 - Information Disclosure Vulnerability in SAP Business One (B1 Client Memory Dump Files) **CVSS Score: 5.8**	In SAP Business One, sensitive information is written to the application□s memory dump files without obfuscation. Gaining access to this information could potentially lead to unauthorized operations within the B1 environment, including modification of company data. This issue results in a high impact on confidentiality and integrity, with no impact on availability.

CVE-2026-24321 - Information Disclosure vulnerability in SAP Commerce Cloud **CVSS Score: 5.3**	SAP Commerce Cloud exposes multiple API endpoints to unauthenticated users, allowing them to submit requests to these open endpoints to retrieve sensitive information that is not intended to be publicly accessible via the front-end. This vulnerability has a low impact on confidentiality and does not affect integrity and availability.
CVE-2026-24312 - Missing authorization check in SAP Business Workflow **CVSS Score: 5.2**	An erroneous authorization check in SAP Business Workflow leads to privilege escalation. An authenticated administrative user can bypass role restrictions by leveraging permissions from a less sensitive function to execute unauthorized, high-privilege actions. This has a high impact on data integrity, with low impact on confidentiality and no impact on availability of the application.
CVE-2026-0486 - Missing Authorization Check in ABAP based SAP systems **CVSS Score: 5.0**	In ABAP based SAP systems a remote enabled function module does not perform necessary authorization checks for an authenticated user resulting in disclosure of system information.This has low impact on confidentiality. Integrity and availability are not impacted.
CVE-2026-24325 - Cross Site Scripting (XSS) vulnerability in SAP BusinessObjects Enterprise (Central Management Console) **CVSS Score: 4.8**	SAP BusinessObjects Enterprise does not sufficiently encode user-controlled inputs, leading to Stored Cross-Site Scripting (XSS) vulnerability. This enables an admin user to inject malicious JavaScript into a website and the injected script gets executed when the user visits the compromised page.This vulnerability has low impact on confidentiality and integrity of the data. There is no impact on the availability of the application.
CVE-2026-23685 - Insecure Deserialization vulnerability in SAP NetWeaver (JMS service) **CVSS Score: 4.4**	Due to a Deserialization vulnerability in SAP NetWeaver (JMS service), an attacker authenticated as an administrator with local access could submit specially crafted content to the server. If processed by the application, this content could trigger unintended behavior during internal logic execution, potentially causing a denial of service. Successful exploitation results in a high impact on availability, while confidentiality and integrity remain unaffected.
CVE-2026-23688 - Missing Authorization check in SAP Fiori App (Manage Service Entry Sheets - Lean Services) **CVSS Score: 4.3**	SAP Fiori App Manage Service Entry Sheets does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This has low impact on integrity, confidentiality and availability are not impacted.
CVE-2026-23681 - Missing Authorization check in a function module in SAP Support Tools Plug-In **CVSS Score: 4.3**	Due to missing authorization check in a function module in SAP Support Tools Plug-In, an authenticated attacker could invoke specific function modules to retrieve information about the system and its configuration. This disclosure of the system information could assist the attacker to plan subsequent attacks. This vulnerability has a low impact on the confidentiality of the application, with no effect on its integrity or availability.
CVE-2026-24326 - Missing authorization check in SAP S/4HANA Defense & Security (Disconnected Operations) **CVSS Score: 4.3**	Due to a missing authorization check in the Disconnected Operations of the SAP S/4HANA Defense & Security, an attacker with user privileges could call remote-enabled function modules to do direct update on standard SAP database table . This results in low impact

	on integrity, with no impact on confidentiality or availability of the application.
CVE-2026-24327 - Missing Authorization Check in SAP Strategic Enterprise Management (Balanced Scorecard in BSP Application) **CVSS Score: 4.3**	Due to missing authorization check in SAP Strategic Enterprise Management (Balanced Scorecard in Business Server Pages), an authenticated attacker could access information that they are otherwise unauthorized to view. This leads to low impact on confidentiality and no effect on integrity or availability.
CVE-2026-23686 - CRLF Injection vulnerability in SAP NetWeaver Application Server Java **CVSS Score: 3.4**	Due to a CRLF Injection vulnerability in SAP NetWeaver Application Server Java, an authenticated attacker with administrative access could submit specially crafted content to the application. If processed by the application, this content enables injection of untrusted entries into generated configuration, allowing manipulation of application-controlled settings. Successful exploitation leads to a low impact on integrity, while confidentiality and availability remain unaffected.
CVE-2026-24327 - Memory Corruption vulnerability in SAP NetWeaver and ABAP Platform (Application Server ABAP) **CVSS Score: 3.1**	Due to improper memory management in SAP NetWeaver and ABAP Platform (Application Server ABAP), an authenticated attacker could exploit logical errors in memory management by supplying specially crafted input containing unique characters, which are improperly converted. This may result in memory corruption and the potential leakage of memory content. Successful exploitation of this vulnerability would have a low impact on the confidentiality of the application, with no effect on its integrity or availability.

***Note**: The VPR scores are not available. Also, there are currently no reports of these vulnerabilities being exploited in the wild.*

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/february-2026.html

CVEs

CVE-2026-0488
CVE-2026-0509
CVE-2026-23687
CVE-2026-23689
CVE-2026-24322
CVE-2026-0490
CVE-2026-0485
CVE-2025-12383
CVE-2026-0508
CVE-2026-0484
CVE-2026-24324
CVE-2026-0505
CVE-2026-24323
CVE-2026-24328
CVE-2025-0059
CVE-2026-23684
CVE-2026-24319
CVE-2026-24321
CVE-2026-24312
CVE-2026-0486
CVE-2026-24325
CVE-2026-23685
CVE-2026-23688
CVE-2026-23681
CVE-2026-24326
CVE-2026-24327
CVE-2026-23686
CVE-2026-24320

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com