Smarttech
YOUR 24/7 SECURITY PARTNER

SAP releases Security Patch – April 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	54
Authors	Daniel-Cristian Carp < daniel.carp@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-04-15
Issue Date	2026-04-14

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 19 new Security Notes. Several of these vulnerabilities are rated Critical (CVSS up to 9.9) or High, addressing severe issues such as SQL injection, code injection, and denial-of-service flaws. If exploited, these vulnerabilities could lead to unauthorized access, data manipulation, system compromise, and disruption of 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 these vulnerabilities are as follows:

CVE ID	***Description***
CVE-2026-27681 - **SQL Injection vulnerability in SAP Business Planning and Consolidation and SAP Business Warehouse** **CVSS Score: 9.9**	Due to insufficient authorization checks in SAP Business Planning and Consolidation and SAP Business Warehouse, an authenticated user can execute crafted SQL statements to read, modify, and delete database data. This leads to a high impact on the confidentiality, integrity, and availability of the system.
CVE-2026-34256 - **Missing Authorization check in SAP ERP and SAP S/4 HANA (Private Cloud and On-Premise)** **CVSS Score: 7.1**	Due to a missing authorization check in SAP ERP and SAP S/4HANA (Private Cloud and On-Premise), an authenticated attacker could execute a particular ABAP report to overwrite any existing eight-character executable ABAP report without authorization. If the overwritten report is subsequently executed, the intended functionality could become unavailable. Successful exploitation impacts availability, with a limited impact on integrity confined to the affected report, while confidentiality remains unaffected.
CVE-2025-64775 - **Denial of Service Vulnerability in SAP**	Denial of Service vulnerability in Apache Struts, file leak in multipart request processing causes disk exhaustion. This issue affects Apache Struts: from 2.0.0 through

BusinessObjects Business Intelligence Platform **CVSS Score: 6.5**	6.7.0, from 7.0.0 through 7.0.3. Users are recommended to upgrade to version 6.8.0 or 7.1.1, which fixes the issue.
CVE-2026-34264 - Information Disclosure vulnerability in SAP Human Capital Management for SAP S/4HANA **CVSS Score: 6.5**	During authorization checks in SAP Human Capital Management for SAP S/4HANA, the system returns specific messages. Due to this, an authenticated user with low privileges could guess and enumerate the content shown, beyond their authorized scope. This leads to disclosure of sensitive information causing a high impact on confidentiality, while integrity and availability are unaffected.
CVE-2026-34261 - Missing Authorization check in SAP Business Analytics and SAP Content Management **CVSS Score: 6.5**	Due to a missing authorization check in SAP Business Analytics and SAP Content Management, an authenticated user could make unauthorized calls to certain remote function modules, potentially accessing sensitive information beyond their intended permissions. This vulnerability affects confidentiality, with no impact on integrity and availability.
CVE-2026-27677 -Missing Authorization check in SAP S/4HANA OData Service (Manage Reference Equipment) **CVSS Score: 6.5**	Due to missing authorization checks in the SAP S/4HANA OData Service (Manage Reference Equipment), an attacker could update and delete child entities via OData services without proper authorization. This vulnerability has a high impact on integrity, while confidentiality and availability are not impacted.
CVE-2026-27678 - Missing Authorization check in SAP S/4HANA Backend OData Service (Manage Reference Structures) **CVSS Score: 6.5**	Due to missing authorization checks in the SAP S/4HANA backend OData Service (Manage Reference Structures), an attacker could update and delete child entities via exposed OData services without proper authorization. This vulnerability has a high impact on integrity, while confidentiality and availability are not impacted.
CVE-2026-27679 - Missing Authorization check in SAP S/4HANA Backend OData Service (Manage Reference Structures) **CVSS Score: 6.5**	Due to missing authorization checks in the SAP S/4HANA frontend OData Service (Manage Reference Structures), an attacker could update and delete child entities via exposed OData services without proper authorization. This vulnerability has a high impact on integrity, while confidentiality and availability are not impacted.
CVE-2026-0512 - Cross-Site Scripting (XSS) vulnerability in SAP Supplier Relationship Management (SICF Handler in SRM Catalog) **CVSS Score: 6.1**	Due to a Cross-Site Scripting (XSS) vulnerability in the SAP Supplier Relationship Management (SICF Handler in SRM Catalog), an unauthenticated attacker could craft a malicious URL, that if accessed by a victim, results in execution of malicious content within the victim's browser. This could allow the attacker to access and modify information, impacting the confidentiality and integrity of the application, while availability remains unaffected.
CVE-2026-27674 - Code Injection vulnerability in SAP NetWeaver Application Server Java (Web Dynpro Java) **CVSS Score: 6.1**	Due to a Code Injection vulnerability in SAP NetWeaver Application Server Java (Web Dynpro Java), an unauthenticated attacker could supply crafted input that is interpreted by the application and causes it to reference attacker-controlled content. If a victim accesses the affected functionality, that attacker-controlled content could be executed in the victim's browser, potentially resulting in session compromise. This could allow the attacker to execute arbitrary client-

	side code, impacting the confidentiality and integrity of the application, with no impact to availability.
CVE-2026-34257 - Open Redirect vulnerability in SAP NetWeaver Application Server ABAP **CVSS Score: 6.1**	Due to an Open Redirect vulnerability in SAP NetWeaver Application Server ABAP, an unauthenticated attacker could craft malicious URL that, if accessed by a victim, they could be redirected to the page controlled by the attacker. This causes low impact on confidentiality and integrity of the application with no impact on availability.
CVE-2026-34262 - Information Disclosure Vulnerability in SAP HANA Cockpit and HANA Database Explorer **CVSS Score: 5.0**	An information disclosure vulnerability exists in SAP HANA Cockpit and SAP HANA Database Explorer that could allow unauthorized access to sensitive information.
CVE-2026-27673 - Missing Authorization Check in SAP S/4HANA (Private Cloud and On-Premise) **CVSS Score: 4.9**	Due to a missing authorization check, SAP S/4HANA (Private Cloud and On-Premise) allows an authenticated user to delete files on the operating system and gain unauthorized control over file operations which could leads to no impact on Confidentiality, Low impact on Integrity and Availability of the application.
CVE-2026-27672 - Missing Authorization check in Material Master Application **CVSS Score: 4.3**	The Material Master application does not enforce authorization checks for authenticated users when executing reports, resulting in the disclosure of sensitive information. This vulnerability has a low impact on confidentiality and does not affect integrity and availability of the system.
CVE-2026-27676 - Missing Authorization check in SAP S/4HANA OData Service (Manage Technical Object Structures) **CVSS Score: 4.3**	Due to missing authorization checks in the SAP S/4HANA OData Service (Manage Technical Object Structures), an attacker could update and delete child entities via exposed OData services without proper authorization. This vulnerability results in a low impact on integrity, while confidentiality and availability are not impacted.
CVE-2025-42899 - Missing Authorization check in SAP S4CORE (Manage Journal Entries) **CVSS Score: 4.3**	SAP S4CORE (Manage journal entries) does not perform necessary authorization checks for an authenticated user resulting in escalation of privileges. This has low impact on confidentiality of the application with no impact on integrity and availability of the application.
CVE-2026-24318 - Insecure Session Management vulnerability in SAP BusinessObjects Business Intelligence Platform **CVSS Score: 4.2**	Due to an Insecure session management vulnerability in SAP Business Objects Business Intelligence Platform, an unauthenticated attacker could obtain valid session tokens and reuse them to gain unauthorized access to a victim's session. If the application continues to accept previously issued tokens after authentication, the attacker could assume the victim's authenticated context. This could allow the attacker to access or modify information within the victim's session scope, impacting confidentiality and integrity, while availability remains unaffected.
CVE-2026-27683 - Reflected cross site scripting vulnerability in SAP BusinessObjects Business Intelligence Platform **CVSS Score: 4.1**	SAP BusinessObjects Business Intelligence application allows an authenticated attacker to inject malicious JavaScript payloads through crafted URLs. When a victim accesses the URL, the script executes in the user's browser, potentially exposing restricted information. This results in a low impact on confidentiality with no impact on integrity and availability.

CVE-2026-27680 - CSS Injection vulnerability in SAP NetWeaver Application Server ABAPCVSS Score: 3.1	The vulnerability associated with CVE-2026-27680 has not yet been disclosed. This CVE ID has been reserved by a CNA, and no impact, severity, or technical details are available at this time.
CVE-2026-27675 - Code Injection vulnerability in SAP Landscape Transformation CVSS Score: 2.0	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.

***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/april-2026.html

CVEs

CVE-2026-27681
CVE-2026-34256
CVE-2025-64775
CVE-2026-34264
CVE-2026-34261
CVE-2026-27677
CVE-2026-27678
CVE-2026-27679
CVE-2026-0512
CVE-2026-27674
CVE-2026-34257
CVE-2026-34262

CVE-2026-27673
CVE-2026-27672
CVE-2026-27676
CVE-2025-42899
CVE-2026-24318
CVE-2026-27683
CVE-2026-27680
CVE-2026-27675

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com