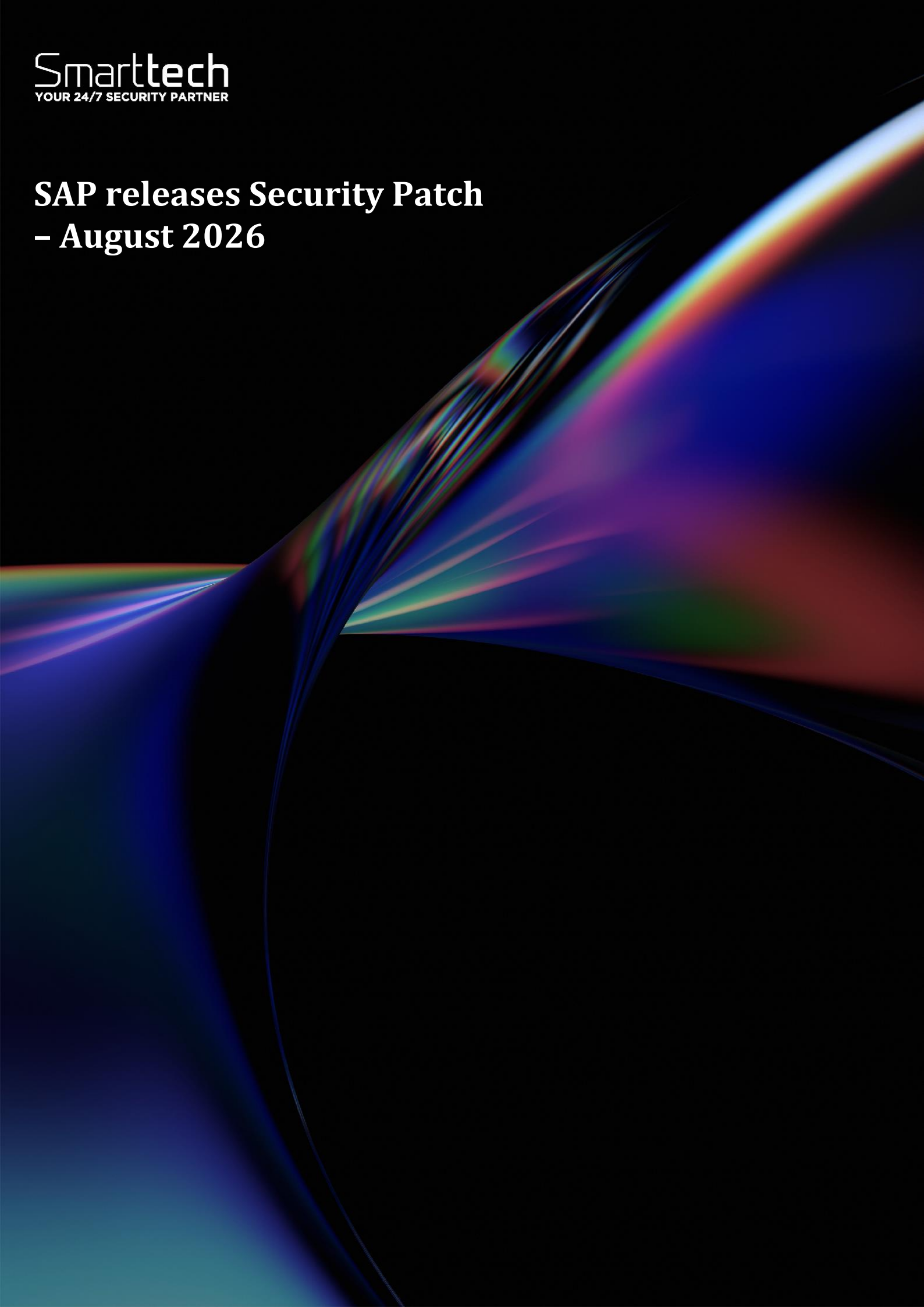
Smarttech
YOUR 24/7 SECURITY PARTNER

SAP releases Security Patch – August 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	131
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-08-11
Issue Date	2026-08-11

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 improper authorization, code injection, memory corruption, privilege escalation, credential disclosure, and directory traversal. If exploited, these vulnerabilities could lead to remote code execution, unauthorized access, privilege escalation, sensitive data exposure, and compromise of system integrity and availability.

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-2026-58231 **CVSS Score: 10** **Improper Authorization in SAP Commerce Cloud (Data Hub Adapter)**	SAP Commerce Cloud allows an unauthenticated attacker to abuse a default authentication client and submit specially crafted input to certain functions lacking sufficient validation. Successful exploitation could enable arbitrary code execution and compromise internal components, resulting in high impact on confidentiality, integrity, and availability of the application.
CVE-2026-44772 **CVSS Score: 9.9** **Code Injection vulnerability in SAP Manufacturing Integration and Intelligence**	The SAP MII Illuminator query servlet accepted three request parameters (InlineTransform, CalculationTransform and StyleSheet) whose value is a URL from which the server fetches an XSL stylesheet. Before the August 2026 patch nothing validated the destination of that URL, so an authenticated user holding ordinary query-execution rights could make the NetWeaver AS Java host issue arbitrary HTTP requests and could have the fetched response body compiled and executed as an XSLT stylesheet inside the server process. A second, cruder endpoint, IllumXSLTServlet, exposed a comparable

	pattern through raw URL and Transform parameters and is corrected separately as CVE-2026-44758.
CVE-2026-34265 **CVSS Score: 9.8** **Memory Corruption vulnerability in Application Server ABAP for SAP NetWeaver and ABAP Platform**	SAP NetWeaver Application Server ABAP allows an unauthenticated attacker to exploit logical errors in DIAG protocol parsing, resulting in memory corruption. This vulnerability could potentially disclose sensitive system information or crash the system, leading to a high impact on the confidentiality, integrity, and availability of the application.
CVE-2026-44758 **CVSS Score: 9.1** **Code Injection vulnerability in Manufacturing Integration and Intelligence**	SAP Manufacturing Integration and Intelligence (MII) allows an attacker with high privileges to submit specially crafted input to certain affected functionality, which is processed without sufficient validation. Successful exploitation could allow the attacker to execute arbitrary commands on the underlying operating system, resulting in high impact on confidentiality, integrity, and availability of the application.
CVE-2026-58243 **CVSS Score: 8.8** **Privilege Escalation vulnerability in SAP ABAP Developer Tools**	SAP ABAP Development Tools does not perform necessary authorization checks for certain functionality, allowing an attacker with low privileges to execute unauthorized database operations against SAP NetWeaver AS ABAP. Successful exploitation could allow the attacker to read sensitive data, modify application data, and disrupt access for legitimate users, resulting in high impact on confidentiality, integrity, and availability.
CVE-2026-42945 **CVSS Score: 8.1** **Potential buffer overflow vulnerability affects SAP Commerce Cloud in public-cloud deployments with NGINX**	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_rewrite_module module. This vulnerability exists when the rewrite directive is followed by a rewrite, if, or set directive and an unnamed Perl-Compatible Regular Expression (PCRE) capture (for example, $1, $2) with a replacement string that includes a question mark (?). An unauthenticated attacker along with conditions beyond its control can exploit this vulnerability by sending crafted HTTP requests. This may cause a heap buffer overflow in the NGINX worker process leading to a restart. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.
CVE-2026-58233 **CVSS Score: 7.6** **Remote Code Execution vulnerability in SAP Change and Transport System Attach Tool (ctsattach)**	SAP Change and Transport System Attach Tool (ctsattach) allows an authenticated attacker to supply a specially crafted archive file which, when processed by the applications library, can trigger insecure deserialization and lead to remote code execution (RCE) on the system. Successful exploitation requires a victim to process the malicious archive, enabling the attacker to execute the RCE and extract sensitive information and gain control over the system and its processes. This vulnerability has a high impact on confidentiality and integrity of the data, with a low impact on the availability of the system.
CVE-2026-66763 **CVSS Score: 7.9** **Credentials disclosure in SAP BusinessObjects Business Intelligence Platform (Central Management Server)**	SAP BusinessObjects Business Intelligence Platform stores certain sensitive credentials associated with user objects using a hard-coded cryptographic key. An attacker with high privileges and local access to the server could retrieve these objects and decrypt the stored credentials. Successful exploitation could allow the attacker to obtain sensitive authentication data and modify protected information, resulting in a high impact on confidentiality and integrity. There is no impact on availability.

CVE-2026-44763 **CVSS Score: 7.6** **Directory Traversal vulnerability in SAP Manufacturing Integration and Intelligence**	SAP Manufacturing Integration and Intelligence allows a privileged attacker to exploit insufficient file path validation in certain functions using specially crafted input. Exploitation also requires a legitimate user to subsequently access the attacker-influenced content and depends on conditions outside the attackers control. Successful exploitation could allow files to be written outside the intended directory and affect other components, resulting in a high impact on confidentiality, integrity, and availability.
CVE-2026-44765 **CVSS Score: 7.3** **Missing Authorization Check in SAP Manufacturing Integration and Intelligence**	Due to a Missing Authorization Check vulnerability in SAP Manufacturing Integration and Intelligence, an unauthenticated remote attacker could access scheduling-related application functions without proper authorization validation. Successful exploitation could allow the attacker to retrieve, create, modify, or delete application-managed scheduling data, causing a low impact on confidentiality, integrity, and availability.
CVE-2026-44764 **CVSS Score: 7.3** **Missing Authorization Check in SAP Manufacturing Integration and Intelligence**	Due to a Missing Authorization Check vulnerability in SAP Manufacturing Integration and Intelligence, an unauthenticated attacker could send crafted requests to the Cost Servlet using specific parameter values. If processed by the application, these requests enable access to backend operations. Successful exploitation could allow the attacker to read, create, modify, or delete application-managed business data, resulting in a limited impact on the confidentiality, integrity, and availability of the affected system.
CVE-2026-58230 **CVSS Score: 7.0** **Multiple vulnerabilities in SAP Business AI Platform (Approuter)**	SAP Approuter does not sufficiently validate certain token content under specific configurations. An unauthenticated attacker could send a specially crafted token to cause sensitive credential material to be sent to an attacker-controlled destination. The attack complexity is high due to non-default preconditions required in the target environment. This results in a high impact on confidentiality and a low impact on integrity and availability.
CVE-2026-58248 **CVSS Score: 6.5** **XML External Entity Injection in SAP BusinessObjects Business Intelligence**	SAP BusinessObjects Business Intelligence Platform (Web Intelligence) allows a low-privileged attacker to upload a specially crafted spreadsheet file containing malicious external references. When the file is processed as a data source, the affected component resolves these references and exposes the contents of sensitive server-side files within the resulting report. This results in a high impact on confidentiality, with no impact on integrity and availability.
CVE-2026-34480 **CVSS Score: 6.5** **Improper Output Encoding Vulnerability in SAP Commerce Cloud and SAP Data Hub (Apache Log4j Core)**	Apache Log4j Core's XmlLayout https://logging.apache.org/log4j/2.x/manual/layouts.html#XmlLayout , in versions up to and including 2.25.3, fails to sanitize characters forbidden by the XML 1.0 specification https://www.w3.org/TR/xml/#charsets producing invalid XML output whenever a log message or MDC value contains such characters. The impact depends on the StAX implementation in use: * JRE built-in StAX: Forbidden characters are silently written to the output, producing malformed XML. Conforming parsers must reject such documents with a fatal error, which may cause downstream log-processing systems to drop the affected records. * Alternative StAX implementations (e.g., Woodstox https://github.com/FasterXML/woodstox , a transitive dependency of the Jackson XML Dataformat module): An

	exception is thrown during the logging call, and the log event is never delivered to its intended appender, only to Log4j's internal status logger. Users are advised to upgrade to Apache Log4j Core 2.25.4, which corrects this issue by sanitizing forbidden characters before XML output.
CVE-2026-5598 **CVSS Score: 6.5** **Potential Information Disclosure vulnerability in SAP Commerce Cloud (Bouncy Castle Java library)**	Covert timing channel vulnerability in Legion of the Bouncy Castle Inc. BC-JAVA core on all (core modules). This vulnerability is associated with program files FrodoEngine.Java. This issue affects BC-JAVA: from 1.71 before 1.80.2, from 1.81 before 1.81.1, from 1.82 before 1.84.
CVE-2026-66779 **CVSS Score: 6.3** **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Application Server ABAP**	Due to a Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Application Server ABAP, an authenticated attacker could generate a malicious link and make it publicly accessible. If an authenticated victim accesses this link, the injected input is processed and reflected within the DOM on the client side during page rendering, resulting in the execution of malicious content in the victim's browser context. Successful exploitation could result in a high impact to the confidentiality and a low impact to the integrity of the system, while availability remains unaffected.
CVE-2026-66770 **CVSS Score: 6.3** **SQL Injection vulnerability in SAP Social Intelligence**	Due to an SQL Injection vulnerability in SAP Social intelligence, an authenticated attacker could directly inject an SQL DDL (Data Definition Language) string into the underlying database without further authorization. Successful exploitation could allow the attacker to make malicious changes to the database structure, resulting in a low impact to the confidentiality, integrity, and availability of the system.
CVE-2026-58235 **CVSS Score: 6.3** **Use of Vulnerable Third-Party Component in SAP NetWeaver AS Java (Adobe Document Services)**	SAP NetWeaver Application Server Java (Adobe Document Service) uses outdated open source cryptographic and data transfer libraries that contain known vulnerabilities addressed in later versions. A low-privileged authenticated attacker could potentially leverage these weaknesses against the affected component, though no specific exploit is currently known. Successful exploitation could result in low impact on confidentiality, integrity, and availability of the system.
CVE-2026-66771 **CVSS Score: 6.1** **Cross Site Scripting (XSS) vulnerability in SAPUI5**	SAPUI5 allows a key user with content adaptation privileges to inject malicious script content into persisted application changes. When another user subsequently opens the adapted application, the injected script executes in the victim's browser session. Successful exploitation could allow the attacker to access sensitive session data and perform unauthorized actions on behalf of the victim, resulting in a high impact on confidentiality and integrity. There is no impact on availability.
CVE-2026-66773 **CVSS Score: 5.9** **Server-controlled `__next` URL is not checking cross-origin**	A malicious or compromised OData service could disclose sensitive authentication information and inject untrusted data into the application, which may leads to a high impact on confidentiality and low impact on integrity and no impact on Availability.
CVE-2026-58236 **CVSS Score: 5.5** **OS Command Injection vulnerability in Application Server ABAP of SAP NetWeaver and ABAP Platform**	SAP NetWeaver Application Server ABAP and ABAP Platform allow an attacker with high privileges to bypass missing security controls on an internal code path leading to operating system command execution. Successful exploitation could allow the attacker to execute OS-level commands that write to the operating system or stop the SAP system, resulting in no impact on confidentiality, low impact on integrity, and high impact on availability.

CVE-2025-42947 **CVSS Score: 5.5** **Code Injection vulnerability in SAP FICA ODN framework**	SAP FICA ODN framework allows a high privileged user to inject value inside the local variable which can then be executed by the application. An attacker could thereby control the behaviour of the application causing high impact on integrity, low impact on availability and no impact on confidentiality of the application.
CVE-2026-40130 **CVSS Score: 5.3** **Memory Corruption vulnerability in SAPSPrint Service**	SAP SAPSPrint Service has memory corruption vulnerabilities in the handling of certain commands. An unauthenticated attacker could send specially crafted requests that trigger a buffer overflow in the affected component. This causes a temporary service interruption and automatic restart, resulting in low impact on availability but no impact on confidentiality and integrity.
CVE-2026-58247 **CVSS Score: 5.3** **Memory Corruption vulnerability in SAP ABAP Platform**	SAP ABAP Platform allows an unauthenticated user to send a specially crafted request to an internal component. This could disclose limited, non-sensitive data from previously used memory, leading to a low on confidentiality, with no impact on integrity and availability of the application.
CVE-2026-33871 **CVE-2025-58057** **CVSS Score: 4.8** **Security Vulnerabilities in SAP Commerce Cloud (Search and Navigation)**	Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In versions prior to 4.1.132.Final and 4.2.10.Final, a remote user can trigger a Denial of Service (DoS) against a Netty HTTP/2 server by sending a flood of `CONTINUATION` frames. The server's lack of a limit on the number of `CONTINUATION` frames, combined with a bypass of existing size-based mitigations using zero-byte frames, allows an user to cause excessive CPU consumption with minimal bandwidth, rendering the server unresponsive. Versions 4.1.132.Final and 4.2.10.Final fix the issue. In netty-codec-compression versions 4.1.124.Final and below, and netty-codec versions 4.2.4.Final and below, when supplied with specially crafted input, BrotliDecoder and certain other decompression decoders will allocate a large number of reachable byte buffers, which can lead to denial of service. BrotliDecoder.decompress has no limit in how often it calls pull, decompressing data 64K bytes at a time. The buffers are saved in the output list, and remain reachable until OOM is hit. This is fixed in versions 4.1.125.Final of netty-codec and 4.2.5.Final of netty-codec-compression.
CVE-2026-66764 **CVSS Score: 4.3** **Missing Authorization check in SAP S/4 HANA (Reprocess Bank Statement Items)**	Reprocess Bank Statement Items in SAP S/4HANA does not perform the necessary authorization checks for authenticated users, allowing them to use rules that have not been shared with them, resulting in privilege escalation.This vulnerability has a low impact on confidentiality, with no impact on integrity and availability of the application
CVE-2026-66772 **CVSS Score: 4.3** **Missing Authorization Check in SAP BusinessObjects Business Intelligence Platform (Admin Tools)**	SAP BusinessObjects Business Intelligence Platform (Admin Tools) does not perform sufficient authorization check on certain administrative functionality. An attacker authenticated as a non-administrative user could bypass this restriction to gain limited information about affected functionality. This results in a low impact on confidentiality. There is no impact on integrity and availability.
CVE-2026-58244 **CVSS Score: 4.3** **Missing Authorization Check in SAP Manufacturing**	SAP Manufacturing Integration and Intelligence (MII) does not perform necessary authorization check on certain application function, allowing a low-privileged authenticated attacker to access information that should be restricted to privileged users. Successful exploitation could allow the attacker to access the

Integration and Intelligence (MII)	users account information in the application, which could be leveraged to facilitate further attacks against the identified user accounts. This vulnerability results in low impact on confidentiality of the data, with no impact on the integrity and availability
CVE-2026-58241 **CVSS Score: 4.2** **Missing Authorization Check in SAP NetWeaver and ABAP Platform (Change and Transport System - Customer Transport Integration Wizard)**	SAP NetWeaver and ABAP Platform (Change and Transport System - Customer Transport Integration Wizard) allows a low-privileged user to modify configuration tables that control access to data objects during specific operations. These unauthorized modifications could result in processing delays and operational disruption, leading to a low impact on the integrity and availability of the application with no impact on confidentiality.
CVE-2026-58245 **CVSS Score: 3.8** **Hard-coded Credentials in SAP Advanced Planning and Optimization (Model Mix Planning)**	SAP Advanced Planning and Optimization (Model Mix Planning) contains a hardcoded credential within the source code of the application to perform authorization check to access certain functionalities in the application. An attacker with high privileges could leverage this hardcoded credential to bypass authorization and delete specific planning-related restrictions in the application. Successful exploitation could result in a low impact on confidentiality and integrity, with no impact on availability of the application.
CVE-2026-44762 **CVSS Score: 3.7** **Security Misconfiguration in SAP Data Services Management Console**	SAP Data Services Management Console allows an overly permissive Content Security Policy (CSP) configuration and lacks certain restrictive directives, which could enable an authenticated malicious user to leverage this weakness in combination with another vulnerability to inject and execute malicious scripts within the application's context. Successful exploitation may result in a low impact on confidentiality and integrity, with no impact on the availability of the application.

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/august-2026.html
https://github.com/p3Nt3st3r-sTAr/CVE-2026-42945-POC

CVEs

CVE-2026-58231
CVE-2026-44772
CVE-2026-34265
CVE-2026-44758
CVE-2026-58243
CVE-2026-42945
CVE-2026-58233
CVE-2026-66763
CVE-2026-44763
CVE-2026-44765
CVE-2026-44764
CVE-2026-58230
CVE-2026-58248
CVE-2026-34480
CVE-2026-5598
CVE-2026-66779
CVE-2026-66770
CVE-2026-58235
CVE-2026-66771
CVE-2026-66773
CVE-2026-58236
CVE-2025-42947
CVE-2026-40130
CVE-2026-58247
CVE-2026-33871
CVE-2025-58057
CVE-2026-66764
CVE-2026-66772
CVE-2026-58244
CVE-2026-58241
CVE-2026-58245
CVE-2026-44762
CVE-2026-66775
CVE-2026-66778
CVE-2026-66760
CVE-2026-66761
CVE-2026-66777
CVE-2026-66776
CVE-2026-66774
CVE-2026-58237
CVE-2026-58238
CVE-2026-58239


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com