Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0485

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in SAP-producten

Publicatiedatum: 12-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (NCSC) verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

SAP heeft meerdere kwetsbaarheden verholpen in diverse SAP-producten, waaronder SAP NetWeaver Application Server ABAP, SAP NetWeaver AS Java, SAP Web Dispatcher, SAP BusinessObjects Business Intelligence Platform, SAP Cloud SDK, SAP Host Agent, SAP NetWeaver Enterprise Portal, SAP NetWeaver Visual Composer, en SAP Solution Tools Plug-In.

Duiding

De kwetsbaarheden betreffen verschillende componenten binnen SAP-producten en omvatten onder andere security misconfiguraties, memory corruptie, OS command injection, broken access control, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Server-Side Request Forgery (SSRF), XML External Entity (XXE) aanvallen, code injection, informatielekken, path traversal, en cryptografische zwaktes. Aanvallers kunnen deze kwetsbaarheden misbruiken om onder meer arbitrary code uit te voeren, denial-of-service te veroorzaken, ongeautoriseerde toegang te verkrijgen, gevoelige informatie te lekken, en integriteit van systemen en data aan te tasten. Sommige kwetsbaarheden vereisen geen authenticatie voor exploitatie, terwijl andere misbruik maken van onvoldoende autorisatie- en inputvalidatiecontroles. De kwetsbaarheden zijn aanwezig in zowel ABAP- als Java-componenten, webinterfaces, en SDK's van SAP. Er zijn geen specifieke aanwijzingen voor publiek beschikbare proof-of-concept exploits in de beschrijvingen, maar de technische details geven aan dat exploitatie mogelijk is via speciaal vervaardigde verzoeken of input.

Oplossingen

SAP heeft updates uitgebracht om de kwetsbaarheden in de genoemde producten te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

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

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-44768	4.1 MEDIUM
CVE-2026-73635	7.5 HIGH
CVE-2026-76964	10.0 CRITICAL
CVE-2026-76965	9.9 CRITICAL
CVE-2026-76966	8.9 HIGH
CVE-2026-76970	7.5 HIGH
CVE-2026-76973	7.5 HIGH
CVE-2026-76976	5.4 MEDIUM
CVE-2026-89103	10.0 CRITICAL
CVE-2026-89114	7.5 HIGH
CVE-2026-89115	4.4 MEDIUM
CVE-2026-89119	9.6 CRITICAL
CVE-2026-89125	6.0 MEDIUM
CVE-2026-89126	10.0 CRITICAL
CVE-2026-89128	5.3 MEDIUM
CVE-2026-89129	5.8 MEDIUM
CVE-2026-89131	4.3 MEDIUM
CVE-2026-109793	7.5 HIGH
CVE-2026-109794	7.5 HIGH
CVE-2026-109795	9.9 CRITICAL
CVE-2026-109796	4.3 MEDIUM
CVE-2026-109797	7.1 HIGH
CVE-2026-109798	9.1 CRITICAL
CVE-2026-109799	7.5 HIGH
CVE-2026-109800	7.7 HIGH
CVE-2026-109801	6.5 MEDIUM
CVE-2026-109802	6.5 MEDIUM
CVE-2026-109803	9.9 CRITICAL

CVE	CVSS Score
CVE-2026-109804	7.5 HIGH
CVE-2026-109805	6.4 MEDIUM
CVE-2026-109806	7.5 HIGH
CVE-2026-109807	7.5 HIGH
CVE-2026-109808	3.1 LOW
CVE-2026-109809	6.5 MEDIUM
CVE-2026-109810	6.1 MEDIUM
CVE-2026-109811	6.5 MEDIUM
CVE-2026-120008	8.2 HIGH
CVE-2026-120009	7.2 HIGH
CVE-2026-120010	7.5 HIGH
CVE-2026-120012	7.5 HIGH
CVE-2026-120013	7.5 HIGH
CVE-2026-120014	7.6 HIGH
CVE-2026-120015	7.5 HIGH
CVE-2026-120016	6.1 MEDIUM
CVE-2026-120017	10.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-15	External Control of System or Configuration Setting
CWE-22	Improper Limitation of a Pathname to a Restricted Directory
CWE-79	Improper Neutralization of Input During Web Page Generation
CWE-94	Improper Control of Generation of Code
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read

CWE	Beschrijving
CWE-131	Incorrect Calculation of Buffer Size
CWE-190	Integer Overflow or Wraparound
CWE-209	Generation of Error Message Containing Sensitive Information
CWE-256	Plaintext Storage of a Password
CWE-294	Authentication Bypass by Capture-replay
CWE-328	Use of Weak Hash
CWE-347	Improper Verification of Cryptographic Signature
CWE-352	Cross-Site Request Forgery
CWE-369	Divide By Zero
CWE-427	Uncontrolled Search Path Element
CWE-522	Insufficiently Protected Credentials
CWE-611	Improper Restriction of XML External Entity Reference
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-749	Exposed Dangerous Method or Function
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write
CWE-835	Loop with Unreachable Exit Condition
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-908	Use of Uninitialized Resource
CWE-918	Server-Side Request Forgery
CWE-942	Permissive Cross-domain Security Policy with Untrusted Domains
CWE-1220	Insufficient Granularity of Access Control
CWE-1287	Improper Validation of Specified Type of Input

Getroffen producten

SAP
CRM WebClient UI
Cloud SDK for AI
Cloud SDK for Python
Gateway
Internet Communication Manager
SAP BusinessObjects Business Intelligence Platform (Web Intelligence)
SAP CRM (WebClient UI)
SAP Host Agent
SAP Kernel
SAP Software
SAP Web Dispatcher
SAP Web Dispatcher and Internet Communication Manager
Software
Web Dispatcher
astonish
message_server
netweaver
web_dispatcher

SAP_SE
S4CRM
SAP ABAP Developer Tools (AMDP Data Preview)
SAP Cloud SDK for AI(JavaScript)
SAP Cloud SDK for Python
SAP Gateway
SAP Solution Tools Plug-In (ST-PI)
SAP Start Service and SAP Microsoft Management Console

SAP_SE
SAP WebClient UI
SAP/astonish

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:
NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.