Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0052

Kwetsbaarheden verholpen in SAP producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-02-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het 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 delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

SAP heeft kwetsbaarheden verholpen in verschillende producten, waaronder SAP CRM, SAP S/4HANA, SAP NetWeaver Application Server ABAP, SAP Supply Chain Management, SAP BusinessObjects BI Platform, SAP Document Management System, SAP Commerce Cloud, en SAP Business Workflow.

Duiding

De kwetsbaarheden omvatten onder andere code-injectie, ontbrekende autorisatiecontroles, Denial of Service, en onjuist beheer van gevoelige informatie. Geauthenticeerde aanvallers kunnen deze kwetsbaarheden misbruiken om ongeautoriseerde toegang te krijgen, gegevensintegriteit te compromitteren, en systeemfunctionaliteit te verstoren. Specifieke kwetsbaarheden kunnen leiden tot ongeautoriseerde SQL-instructies, manipulatie van XML-documenten, en privilege-escalatie. De impact varieert van risico's voor vertrouwelijkheid en integriteit tot verstoring van systeemdiensten.

Oplossingen

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

Referenties

- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/february-2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-0488	8.7 HIGH
CVE-2026-0509	5.3 MEDIUM
CVE-2026-23687	5.3 MEDIUM
CVE-2026-23689	7.1 HIGH
CVE-2026-24322	5.3 MEDIUM
CVE-2026-0490	8.7 HIGH

CVE-2026-0485	6.9 MEDIUM
CVE-2025-12383	9.4 CRITICAL
CVE-2026-0508	2.0 LOW
CVE-2026-0484	5.1 MEDIUM
CVE-2026-24324	7.1 HIGH
CVE-2026-0505	5.3 MEDIUM
CVE-2026-24323	5.3 MEDIUM
CVE-2026-24328	5.3 MEDIUM
CVE-2025-0059	6.0 MEDIUM
CVE-2026-23684	6.3 MEDIUM
CVE-2026-24319	4.6 MEDIUM
CVE-2026-24321	6.9 MEDIUM
CVE-2026-24312	5.1 MEDIUM
CVE-2026-0486	5.3 MEDIUM
CVE-2026-24325	4.8 MEDIUM
CVE-2026-23685	4.6 MEDIUM
CVE-2026-23688	5.3 MEDIUM
CVE-2026-23681	5.3 MEDIUM
CVE-2026-24326	5.3 MEDIUM
CVE-2026-24327	5.3 MEDIUM
CVE-2026-23686	4.8 MEDIUM
CVE-2026-24320	2.3 LOW

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')
CWE-296	Improper Following of a Certificate's Chain of Trust
CWE-316	Cleartext Storage of Sensitive Information in Memory
CWE-347	Improper Verification of Cryptographic Signature
CWE-359	Exposure of Private Personal Information to an Unauthorized Actor
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-366	Race Condition within a Thread
CWE-405	Asymmetric Resource Consumption (Amplification)
CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
CWE-502	Deserialization of Untrusted Data
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-606	Unchecked Input for Loop Condition
CWE-862	Missing Authorization
CWE-937	CWE-937
CWE-1035	CWE-1035

Getroffen producten

SAP
ABAP

Business One
Business Server Pages Application
Business Workflow
BusinessObjects BI Platform
BusinessObjects Business Intelligence Platform
BusinessObjects Enterprise
CRM and S4HANA
Commerce Cloud
Document Management System
Fiori App
NetWeaver
NetWeaver AS ABAP and ABAP Platform
NetWeaver Application Server ABAP and ABAP Platform
NetWeaver Application Server ABAP and S-4HANA
NetWeaver Application Server Java
NetWeaver and ABAP Platform

S4HANA Defense & Security
SAP Software
Solution Tools Plug-In
Strategic Enterprise Management
Supply Chain Management
Support Tools Plug-In

Disclaimer