Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0113

Kwetsbaarheden verholpen in SAP-producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 14-04-2026

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 SAP-producten, waaronder SAP Supplier Relationship Management, SAP BusinessObjects Business Intelligence Platform, SAP NetWeaver Application Server Java en ABAP, SAP Landscape Transformation, SAP Business Planning and Consolidation, SAP Business Warehouse, SAP Content Management en SAP Human Capital Management.

Duiding

De kwetsbaarheden betreffen onder andere Cross-Site Scripting (XSS), code-injectie- en open redirect-kwetsbaarheden die misbruik door ongeauthenticeerde aanvallers mogelijk maken. Verder zijn er SQL-injectieproblemen in SAP Business Planning and Consolidation en SAP Business Warehouse. De kwetsbaarheden beïnvloeden de vertrouwelijkheid, integriteit en beschikbaarheid van data en systemen.

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/april-2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-0512	5.3 MEDIUM
CVE-2026-24318	2.3 LOW
CVE-2026-27672	4.3 MEDIUM
CVE-2026-27673	4.9 MEDIUM
CVE-2026-27674	6.1 MEDIUM
CVE-2026-27675	2.0 LOW
CVE-2026-27676	5.3 MEDIUM

CVE-2026-27677	**5.3 MEDIUM**
CVE-2026-27678	**5.3 MEDIUM**
CVE-2026-27679	**5.3 MEDIUM**
CVE-2026-27680	
CVE-2026-27681	**5.3 MEDIUM**
CVE-2026-27683	**5.1 MEDIUM**
CVE-2026-34256	**5.3 MEDIUM**
CVE-2026-34257	**6.1 MEDIUM**
CVE-2026-34261	**5.3 MEDIUM**
CVE-2026-34262	**5.3 MEDIUM**
CVE-2026-34264	**5.3 MEDIUM**

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-204	Observable Response Discrepancy
CWE-522	Insufficiently Protected Credentials
CWE-539	Use of Persistent Cookies Containing Sensitive Information
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-862	Missing Authorization

Getroffen producten

SAP
Business Analytics, Content Management
Business Planning and Consolidation and Business Warehouse
BusinessObjects Business Intelligence Platform
ERP, S4 HANA
HANA Cockpit, HANA Database Explorer
Human Capital Management for S4HANA
S4HANA Backend OData Service
S4HANA Frontend OData Service
S4HANA OData Service
SAP BusinessObjects Business Intelligence Platform
SAP NetWeaver Application Server ABAP
SAP Software
Supplier Relationship Management
SAP_SE
Material Master Application

SAP Business Analytics and SAP Content Management
SAP Business Planning and Consolidation and SAP Business Warehouse
SAP ERP and SAP S/4 HANA (Private Cloud and On-Premise)
SAP HANA Cockpit and HANA Database Explorer
SAP Human Capital Management for SAP S/4HANA
SAP Landscape Transformation
SAP NetWeaver Application Server Java (Web Dynpro Java)
SAP S/4HANA (Private Cloud and On-Premise)
SAP S/4HANA Backend OData Service (Manage Reference Structures)
SAP S/4HANA Frontend OData Service (Manage Reference Structures)
SAP S/4HANA OData Service (Manage Reference Equipment)
SAP S/4HANA OData Service (Manage Technical Object Structures)
SAP Supplier Relationship Management (SICF Handler in SRM Catalog)

Disclaimer