



NCSC-2026-0230

Kwetsbaarheden verholpen in SAP-producten

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 17-07-2026

Revisie: 1.0.1

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

Update Revisie 1

Door een verwerkingsfout zijn aan de oorspronkelijke advisory geen referenties meegegeven. Dit is hersteld. De advisory is inhoudelijk niet veranderd.

Feiten

SAP heeft kwetsbaarheden verholpen in SAP NetWeaver Application Server ABAP, SAP Approuter, SAP Commerce Cloud, SAP NetWeaver Application Server Java, SAProuter, SAP Change and Transport System Attach Tool, SAP NetWeaver Enterprise Portal, SAP S/4HANA modules, SAP Fiori Launchpad, SAP CRM WebClient UI, SAP HANA Database user self service tools, en SAP Commerce Cloud.

Update: Door een verwerkingsfout waren geen referenties meegegeven. Dit is hersteld. Er zijn verder geen inhoudelijke wijzigingen

Duiding

De kwetsbaarheden betreffen diverse beveiligingsproblemen zoals:

- geheugenbeschadiging in SAP NetWeaver Application Server ABAP
- HTTP Request Smuggling in SAP Approuter
- onveilige OAuth2-sample credentials in SAP Commerce Cloud
- directory traversal in SAP NetWeaver Application Server Java
- DLL hijacking in SAProuter op Windows.
- Verder zijn er Cross-Site Scripting (XSS) kwetsbaarheden in SAP NetWeaver Application Server Java en Enterprise Portal en ontbrekende autorisatiecontroles in SAP S/4HANA modules.
- SAP Change and Transport System Attach Tool is kwetsbaar voor remote code execution door onveilige deserialisatie.
- SAP HANA user self service tools maken informatieoverdracht mogelijk zonder authenticatie.

De kwetsbaarheden kunnen leiden tot ongeautoriseerde toegang, manipulatie van data, informatielekken, en verstoring van de beschikbaarheid. Sommige kwetsbaarheden vereisen authenticatie, andere kunnen door onbevoegden worden misbruikt. Diverse kwetsbaarheden zijn specifiek voor componenten die binnen SAP-omgevingen worden gebruikt, zoals Apache Camel binnen de SAP Integration Suite en Apache Tomcat binnen SAP Commerce Cloud.

Oplossingen

SAP heeft updates uitgebracht om de genoemde kwetsbaarheden te verhelpen. Gebruikers van de getroffen SAP-producten wordt geadviseerd deze updates te installeren om de beveiligingsproblemen te mitigeren. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://support.sap.com/en/my-support/knowledge-base/security-notes-news/july-2026.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-44747	8.7 HIGH
➤ CVE-2026-27690	6.9 MEDIUM
➤ CVE-2026-44761	6.9 MEDIUM
➤ CVE-2026-40128	9.0 CRITICAL
➤ CVE-2026-40860	5.3 MEDIUM
➤ CVE-2026-0487	7.3 HIGH
➤ CVE-2026-44752	5.3 MEDIUM
➤ CVE-2026-44745	5.3 MEDIUM
➤ CVE-2026-43512	9.8 CRITICAL
➤ CVE-2026-41293	9.8 CRITICAL
➤ CVE-2026-43515	9.1 CRITICAL
➤ CVE-2026-58233	5.1 MEDIUM
➤ CVE-2026-44759	5.3 MEDIUM
➤ CVE-2026-44767	5.3 MEDIUM
➤ CVE-2026-44769	5.1 MEDIUM
➤ CVE-2026-44760	5.3 MEDIUM
➤ CVE-2026-44771	5.3 MEDIUM
➤ CVE-2026-44770	5.3 MEDIUM

> CVE-2026-24315	4.2 MEDIUM
> CVE-2026-44768	2.3 LOW
> CVE-2026-44753	6.9 MEDIUM
> CVE-2025-68161	6.3 MEDIUM
> CVE-2026-40453	5.3 MEDIUM
> CVE-2026-33454	6.9 MEDIUM

CWE's

CWE	Beschrijving
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor

Getroffen producten

SAP
CRM WebClient UI
Change and Transport System Attach Tool
Commerce Cloud
HANA Database
NetWeaver Application Server ABAP
NetWeaver Application Server Java
NetWeaver Enterprise Portal

S4 HANA
SAP Commerce Cloud
SAP NetWeaver Application Server ABAP
SAP NetWeaver Enterprise Portal
SAP Software

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.