



NCSC-2026-0091

Kwetsbaarheden verholpen in SAP-producten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 12-03-2026

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 Quotation Management Insurance en SAP NetWeaver. Een deel van de verholpen kwetsbaarheden bevindt zich in producten van derde partijen - zoals Oracle - die verwerkt zitten in SAP producten.

Duiding

De kwetsbaarheden omvatten onder andere een code-injectie flaw, ontbrekende autorisatiecontroles, Denial of Service, een DOM-gebaseerde Cross-Site Scripting (XSS) en onjuist beheer van gevoelige informatie. Deze kwetsbaarheden kunnen worden misbruikt om toegang te krijgen tot gevoelige informatie, ongeautoriseerde wijzigingen aan te brengen of zelfs code-uitvoering te veroorzaken. De kwetsbaarheden hebben invloed op de beschikbaarheid, vertrouwelijkheid en integriteit van de systemen, afhankelijk van de specifieke kwetsbaarheid.

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/march-2026.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2019-17571	9.8 CRITICAL
➤ CVE-2025-9230	6.9 MEDIUM
➤ CVE-2025-9232	6.3 MEDIUM
➤ CVE-2026-0489	5.3 MEDIUM
➤ CVE-2026-24309	5.3 MEDIUM
➤ CVE-2026-24310	2.3 LOW
➤ CVE-2026-24311	1.0 LOW

> CVE-2026-24313	5.3 MEDIUM
> CVE-2026-24316	5.3 MEDIUM
> CVE-2026-24317	7.3 HIGH
> CVE-2026-27684	5.3 MEDIUM
> CVE-2026-27685	8.6 HIGH
> CVE-2026-27686	2.3 LOW
> CVE-2026-27687	2.1 LOW
> CVE-2026-27688	5.3 MEDIUM
> CVE-2026-27689	7.1 HIGH

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-125	Out-of-bounds Read
> CWE-312	Cleartext Storage of Sensitive Information
> CWE-427	Uncontrolled Search Path Element
> CWE-502	Deserialization of Untrusted Data
> CWE-606	Unchecked Input for Loop Condition
> CWE-787	Out-of-bounds Write
> CWE-862	Missing Authorization
> CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

SAP
NetWeaver
NetWeaver Application Server for ABAP
NetWeaver Enterprise Portal Administration
S4HANA HCM Portugal, ERP HCM Portugal
Supply Chain Management
SAP_SE
SAP Business One (Job Service)
SAP Business Warehouse (Service API)
SAP GUI for Windows with active GuiXT
SAP NetWeaver (Feedback Notification)

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.