



NCSC-2025-0076

Kwetsbaarheden verholpen in SAP software

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 11-03-2025

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 meerdere kwetsbaarheden verholpen in zijn softwarecomponenten, waaronder SAP Commerce, SAP NetWeaver, en SAP BusinessObjects.

Duiding

De kwetsbaarheden omvatten onder andere Cross-Site Scripting (XSS) en ontbrekende autorisatiecontroles, die aanvallers in staat stellen om ongeautoriseerde toegang te verkrijgen, gegevens te manipuleren en gevoelige informatie te onthullen. Deze kwetsbaarheden kunnen leiden tot ernstige gevolgen voor de integriteit en vertrouwelijkheid van de gegevens binnen de getroffen systemen. Specifieke kwetsbaarheden zijn onder andere het ontbreken van essentiële autorisatiecontroles in SAP NetWeaver en de mogelijkheid voor aanvallers om sessies te stelen via de SAP Approuter Node.js package.

Oplossingen

SAP heeft updates uitgebracht om de kwetsbaarheden te verhelpen, waaronder 21 beveiligingspatches voor de SAP Approuter en andere kritieke kwetsbaarheden. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://support.sap.com/en/my-support/knowledge-base/security-notes-news/march-2025.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-27434	8.8 HIGH
➤ CVE-2025-26661	8.8 HIGH
➤ CVE-2024-38286	7.7 HIGH
➤ CVE-2025-24876	5.3 MEDIUM
➤ CVE-2024-39592	7.7 HIGH
➤ CVE-2025-26658	6.8 MEDIUM
➤ CVE-2025-26659	6.1 MEDIUM

> CVE-2025-25242	6.1 MEDIUM
> CVE-2025-25244	5.7 MEDIUM
> CVE-2025-27431	5.4 MEDIUM
> CVE-2025-25245	5.4 MEDIUM
> CVE-2025-23194	5.3 MEDIUM
> CVE-2025-0071	4.9 MEDIUM
> CVE-2025-0062	4.7 MEDIUM
> CVE-2025-27433	4.3 MEDIUM
> CVE-2025-23188	4.3 MEDIUM
> CVE-2025-26660	4.3 MEDIUM
> CVE-2025-26656	4.3 MEDIUM
> CVE-2024-41736	4.3 MEDIUM
> CVE-2025-23185	4.1 MEDIUM
> CVE-2024-38819	6.9 MEDIUM
> CVE-2025-27430	3.5 LOW
> CVE-2025-26655	3.1 LOW
> CVE-2025-27432	2.4 LOW

CWE's

CWE	Beschrijving
> CVE-302	Authentication Bypass by Assumed-Immutable Data
> CVE-1287	Improper Validation of Specified Type of Input
> CVE-601	URL Redirection to Untrusted Site ('Open Redirect')
> CVE-532	Insertion of Sensitive Information into Log File

➤ CWE-639	Authorization Bypass Through User-Controlled Key
➤ CWE-306	Missing Authentication for Critical Function
➤ CWE-862	Missing Authorization
➤ CWE-400	Uncontrolled Resource Consumption
➤ CWE-770	Allocation of Resources Without Limits or Throttling
➤ CWE-918	Server-Side Request Forgery (SSRF)
➤ CWE-384	Session Fixation
➤ CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
➤ CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
➤ CWE-209	Generation of Error Message Containing Sensitive Information
➤ CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

SAP
SAP Software
SAP_SE
SAP Commerce (Swagger UI)
SAP NetWeaver (ABAP Class Builder)
SAP Approuter Node.js package
SAP Business One (Service Layer)

SAP Business Warehouse (Process Chains)
SAP Web Dispatcher and Internet Communication Manager
SAP BusinessObjects Business Intelligence Platform (Web Intelligence)
SAP S/4HANA (Manage Bank Statements)
SAP S/4HANA (RBD)
SAP Fiori apps (Posting Library)
S/4HANA (Manage Purchasing Info Records)
SAP Business Objects Business Intelligence Platform
SAP BusinessObjects Business Intelligence Platform
SAP CRM and SAP S/4HANA (Interaction Center)
SAP Electronic Invoicing for Brazil (eDocument Cockpit)
SAP Just In Time
SAP NetWeaver Application Server ABAP

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.