



NCSC-2025-0275

Kwetsbaarheden verholpen in SAP producten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 09-09-2025

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 kwetsbaarheden verholpen in verschillende producten, waaronder in SAP NetWeaver, SAP NetWeaver Application Server Java en SAP Landscape Transformation.

Duiding

De kwetsbaarheden bevinden zich onder andere in de RMI-P4 module en de SAP NetWeaver AS Java platform.

De kwetsbaarheid met kenmerk CVE-2025-42944 betreft een deserialisatieprobleem dat kan worden misbruikt door niet-geauthenticeerde aanvallers, wat kan leiden tot willekeurige OS-commando-executie. Dit bedreigt de vertrouwelijkheid, integriteit en beschikbaarheid van de applicatie.

De kwetsbaarheid met kenmerk CVE-2025-42922 stelt geauthenticeerde niet-administratieve gebruikers in staat om willekeurige bestanden te uploaden via de Deploy Web Service-functie. Dit kan ook leiden tot compromittering van systeemvertrouwelijkheid, integriteit en beschikbaarheid.

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/september-2025.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2023-5072	7.5 HIGH
➤ CVE-2023-27500	9.6 CRITICAL
➤ CVE-2024-13009	
➤ CVE-2025-22228	6.3 MEDIUM
➤ CVE-2025-27428	5.3 MEDIUM
➤ CVE-2025-42911	5.3 MEDIUM

> CVE-2025-42912	5.3 MEDIUM
> CVE-2025-42913	2.3 LOW
> CVE-2025-42914	2.3 LOW
> CVE-2025-42915	5.3 MEDIUM
> CVE-2025-42916	4.8 MEDIUM
> CVE-2025-42917	5.3 MEDIUM
> CVE-2025-42918	5.3 MEDIUM
> CVE-2025-42920	5.3 MEDIUM
> CVE-2025-42922	8.7 HIGH
> CVE-2025-42923	5.1 MEDIUM
> CVE-2025-42925	5.3 MEDIUM
> CVE-2025-42926	6.9 MEDIUM
> CVE-2025-42927	4.6 MEDIUM
> CVE-2025-42929	4.8 MEDIUM
> CVE-2025-42930	7.1 HIGH
> CVE-2025-42933	5.3 MEDIUM
> CVE-2025-42938	5.3 MEDIUM
> CVE-2025-42941	4.8 MEDIUM
> CVE-2025-42944	9.3 CRITICAL
> CVE-2025-42958	8.6 HIGH
> CVE-2025-42961	5.1 MEDIUM

CWE's

CWE	Beschrijving
> CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CWE-94	Improper Control of Generation of Code ('Code Injection')
> CWE-250	Execution with Unnecessary Privileges
> CWE-287	Improper Authentication
> CWE-306	Missing Authentication for Critical Function
> CWE-341	Predictable from Observable State
> CWE-352	Cross-Site Request Forgery (CSRF)
> CWE-404	Improper Resource Shutdown or Release
> CWE-502	Deserialization of Untrusted Data
> CWE-521	Weak Password Requirements
> CWE-522	Insufficiently Protected Credentials
> CWE-606	Unchecked Input for Loop Condition
> CWE-770	Allocation of Resources Without Limits or Throttling
> CWE-862	Missing Authorization
> CWE-863	Incorrect Authorization
> CWE-1022	Use of Web Link to Untrusted Target with window.opener Access
> CWE-1287	Improper Validation of Specified Type of Input
> CWE-1395	Dependency on Vulnerable Third-Party Component

Getroffen producten

SAP
Business Planning and Consolidation
NetWeaver ABAP Platform
NetWeaver AS Java
Netweaver
SAP Business One (SLD)
SAP Fiori (Launchpad)
SAP Fiori App (F4044 Manage Work Center Groups)
SAP HCM (Approve Timesheets Fiori 2.0 application)
SAP HCM (My Timesheet Fiori 2.0 application)
SAP Landscape Transformation Replication Server
SAP NetWeaver (Service Data Download)
SAP NetWeaver AS Java (Adobe Document Service)
SAP NetWeaver AS Java (Deploy Web Service)
SAP NetWeaver AS Java (IIOP Service)
SAP NetWeaver Application Server Java

SAP NetWeaver Application Server for ABAP
SAP NetWeaver Application Server for ABAP (Background Processing)
SAP NetWeaver and ABAP Platform (Service Data Collection)
SAP Netweaver (RMI-P4)
SAP S/4HANA (Private Cloud or On-Premise)
Supplier Relationship Management

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 or 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.