



# NCSC-2025-0323

## Kwetsbaarheden verholpen in SAP Producten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 17-10-2025

**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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

SAP heeft kwetsbaarheden verholpen in diverse SAP producten.

## Duiding

De kwetsbaarheden omvatten een deserialisatie kwetsbaarheid die ongeauthenticeerde aanvallers in staat stelt om willekeurige OS-commando's uit te voeren, en een CSRF-kwetsbaarheid die geauthenticeerde aanvallers in staat stelt om kritieke autorisatiecontroles te omzeilen. Daarnaast zijn er kwetsbaarheden die leiden tot ongeautoriseerde toegang tot gevoelige ABAP-code en de mogelijkheid om verwerkingsregels te verwijderen zonder de juiste autorisatie. Deze kwetsbaarheden kunnen leiden tot ernstige gevolgen voor de integriteit en vertrouwelijkheid van de applicatie.

## Oplossingen

SAP heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

## Kwetsbaarheden

CVE	CVSS Score
<a href="#">&gt; CVE-2025-42944</a>	9.3 CRITICAL
<a href="#">&gt; CVE-2025-42937</a>	6.9 MEDIUM
<a href="#">&gt; CVE-2025-42910</a>	5.3 MEDIUM
<a href="#">&gt; CVE-2025-5115</a>	7.7 HIGH
<a href="#">&gt; CVE-2025-48913</a>	6.3 MEDIUM
<a href="#">&gt; CVE-2025-0059</a>	6.0 MEDIUM
<a href="#">&gt; CVE-2025-42901</a>	5.1 MEDIUM
<a href="#">&gt; CVE-2025-42908</a>	5.3 MEDIUM
<a href="#">&gt; CVE-2025-42906</a>	6.9 MEDIUM
<a href="#">&gt; CVE-2025-42902</a>	6.9 MEDIUM

> CVE-2025-42939	5.3 MEDIUM
> CVE-2025-31331	4.3 MEDIUM
> CVE-2025-42903	5.3 MEDIUM
> CVE-2025-31672	6.9 MEDIUM
> CVE-2025-42909	6.3 MEDIUM

## CWE's

CWE	Beschrijving
> CWE-20	Improper Input Validation
> CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CWE-35	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-204	Observable Response Discrepancy
> CWE-352	Cross-Site Request Forgery (CSRF)
> CWE-400	Uncontrolled Resource Consumption
> CWE-434	Unrestricted Upload of File with Dangerous Type
> CWE-476	NULL Pointer Dereference
> CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
> CWE-502	Deserialization of Untrusted Data
> CWE-770	Allocation of Resources Without Limits or Throttling
> CWE-863	Incorrect Authorization
> CWE-1004	Sensitive Cookie Without 'HttpOnly' Flag

## Getroffen producten

<b>SAP</b>
Application Server for ABAP
Cloud Appliance Library Appliances
Commerce Cloud
Financial Service Claims Management
NetWeaver Application Server for ABAP
Netweaver
Netweaver AS ABAP and ABAP Platform
Print Service
S4HANA
SAP Commerce Cloud
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 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.