Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op 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
CVE-2025-42944	9.3 CRITICAL
CVE-2025-42937	6.9 MEDIUM
CVE-2025-42910	5.3 MEDIUM
CVE-2025-5115	7.7 HIGH
CVE-2025-48913	6.3 MEDIUM
CVE-2025-0059	6.0 MEDIUM
CVE-2025-42901	5.1 MEDIUM
CVE-2025-42908	5.3 MEDIUM
CVE-2025-42906	6.9 MEDIUM
CVE-2025-42902	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

SAP
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