Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0472

Kwetsbaarheden verholpen in SAP producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-12-2024

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 SAP NetWeaver, ABAP, Web Dispatcher, Business Objects, HCM en Commerce Cloud.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Cross-Site-Scripting (XSS)
- Server-Side Request Forgery (SSRF)
- Manipulatie van gegevens
- Omzeilen van een beveiligingsmaatregel
- Uitvoer van willekeurige code (gebruikersrechten)
- Toegang tot gevoelige gegevens

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/december-2024.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-32732	5.3 MEDIUM
CVE-2024-47576	3.3 LOW
CVE-2024-47577	2.7 LOW
CVE-2024-47578	9.1 CRITICAL
CVE-2024-47579	6.8 MEDIUM
CVE-2024-47580	6.8 MEDIUM

CVE-2024-47581	4.3 MEDIUM
CVE-2024-47582	
CVE-2024-47585	4.3 MEDIUM
CVE-2024-47586	5.3 MEDIUM
CVE-2024-47590	8.8 HIGH
CVE-2024-54197	
CVE-2024-54198	8.5 HIGH

CWE's

CWE	Beschrijving
CWE-914	Improper Control of Dynamically-Identified Variables
CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
CWE-791	Incomplete Filtering of Special Elements
CWE-427	Uncontrolled Search Path Element
CWE-319	Cleartext Transmission of Sensitive Information
CWE-862	Missing Authorization
CWE-476	NULL Pointer Dereference
CWE-918	Server-Side Request Forgery (SSRF)
CWE-611	Improper Restriction of XML External Entity Reference
CWE-538	Insertion of Sensitive Information into Externally-Accessible File or Directory

Getroffen producten

sap
businessobjects_business_intelligence_platform
commerce_cloud
hcm
netweaver_abap_application_server
netweaver_administrator
netweaver_application_server_abap
netweaver_as_for_java
netweaver_as_java
product_lifecycle_costing
sap
web_dispatcher
sap_se
sap_businessobjects_business_intelligence_platform
sap_commerce_cloud
sap_hcm
sap_netweaver_administrator_system_overview_
sap_netweaver_application_server_abap
sap_netweaver_application_server_for_abap_and_abap_platform
sap_netweaver_as_for_java__adobe_document_services_
sap_netweaver_as_java
sap_product_lifecycle_costing
sap_web_dispatcher

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.