Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0356

Kwetsbaarheden verholpen in diverse SAP-producten

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-09-2026

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 Extended Passport Protocol (EPP) processing library, SAP NetWeaver Message Server, @sap/cds-mtxs NPM library, SAP GUI for Java, SAP ABAP Development Tools voor SAP NetWeaver AS ABAP, SAP Integration Suite, SAP NetWeaver Business Client, SAP Web Dispatcher, Internet Communication Manager, SAP Content Server, SAP S/4HANA Intercompany Matching and Reconciliation module, en SAP Manufacturing Integration and Intelligence.

Duiding

De kwetsbaarheid met kenmerk CVE-2026-44756 heeft CVSS-score van 10. Het betreft een geheugenveiligheidsprobleem in de EPP processing library dat kan worden geactiveerd door niet-geauthenticeerde aanvallers die malformed EPP headers versturen. Deze geheugenbeschadiging kan leiden tot ongedefinieerd gedrag, wat de vertrouwelijkheid, integriteit en beschikbaarheid van de applicatie kan beïnvloeden. De kwetsbaarheid ontstaat door onjuiste verwerking van EPP headers binnen de SAP EPP processing library. Exploitatie vereist geen authenticatie.

De kwetsbaarheid met kenmerk CVE-2026-58240 heeft CVSS-score van 9.8. Het betreft het ontbreken van een authenticatiemechanisme bij de registratie van interne applicatieservercomponenten. Hierdoor valideert het systeem niet correct of de componenten legitiem zijn. Een niet-geauthenticeerde aanvaller met netwerktoegang kan hierdoor ongeautoriseerde componenten registreren binnen de Message Server-omgeving. Dit kan leiden tot compromittering van de vertrouwelijkheid, integriteit en beschikbaarheid van de getroffen SAP NetWeaver-systemen.

De kwetsbaarheid met kenmerk CVE-2026-76969 heeft CVSS-score van 9.4. De kwetsbaarheid maakt het mogelijk voor niet-geauthenticeerde aanvallers om gevoelige credentials te verkrijgen. Dit kan leiden tot ongeautoriseerde toegang en manipulatie van tenantgegevens. De kwetsbaarheid betreft credential disclosure in multitenant CAP-applicaties en beïnvloedt de vertrouwelijkheid, integriteit en beschikbaarheid van de getroffen systemen.

De kwetsbaarheid met kenmerk CVE-2026-66768 heeft CVSS-score van 9.0. De kwetsbaarheid betreft een onjuiste toegangcontrole en het niet correct afdwingen van trust level policies in SAP GUI for Java. Hierdoor kan een aanvaller met lage privileges willekeurige commando's uitvoeren door misbruik te maken van zwakheden in de backend verwerking van trust policies. Dit beïnvloedt de integriteit van het beveiligingsmodel van het systeem.

De overige kwetsbaarheden variëren in ernst van middelmatig tot hoog en betreffen diverse beveiligingsproblemen zoals:

- niet juist uitvoeren van autorisatiecontroles in SAP ABAP Developer Tools
- XML External Entity (XXE) in SAP Integration Suite
- onveilige deserialisatie in SAP NetWeaver Business Client

- geheugenbeschadiging in SAP NetWeaver Application Server for ABAP en ABAP Platform
- CRLF-injectie door het gebruik van Jetty-componenten in SAP Commerce Cloud
- informatielek in SAP Web Dispatcher, Internet Communication Manager en SAP Content Server
- SQL-injectie in SAP S/4HANA (Intercompany Matching and Reconciliation)
- Server-Side Request Forgery (SSRF) in SAP Manufacturing Integration and Intelligence

Deze kwetsbaarheden kunnen leiden tot privilege-escalatie, ongeautoriseerde toegang, informatielekken, gegevensmanipulatie en verstoring van de beschikbaarheid. Meerdere kwetsbaarheden kunnen zonder authenticatie worden uitgebuit. De kwetsbaarheden treffen diverse SAP-componenten, waaronder SAP ABAP Developer Tools, SAP Integration Suite, SAP NetWeaver, SAP Commerce Cloud, SAP Web Dispatcher, SAP S/4HANA en SAP Manufacturing Integration and Intelligence.

Oplossingen

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

Referenties

- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/september-2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-44756	10.0 CRITICAL
CVE-2026-58240	9.8 CRITICAL
CVE-2026-76969	9.4 CRITICAL
CVE-2026-66768	9.0 CRITICAL
CVE-2026-58243	8.8 HIGH
CVE-2026-76958	8.5 HIGH
CVE-2026-76967	7.8 HIGH
CVE-2026-76968	6.5 MEDIUM
CVE-2026-44766	6.5 MEDIUM

CVE-2026-76971	6.5 MEDIUM
CVE-2026-2332	9.1 CRITICAL

CWE's

CWE	Beschrijving
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-308	Use of Single-factor Authentication
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
CWE-502	Deserialization of Untrusted Data
CWE-522	Insufficiently Protected Credentials
CWE-611	Improper Restriction of XML External Entity Reference
CWE-807	Reliance on Untrusted Inputs in a Security Decision
CWE-862	Missing Authorization
CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

SAP
Content Server, Internet Communication Manager, Web Dispatcher
Extended Passport Processing

GUI for Java
Integration Suite
Manufacturing Integration and Intelligence
NetWeaver
NetWeaver Business Client
NetWeaver Message Server
S4HANA
SAP Software
netweaver
SAP_SE
SAP ABAP Developer Tools
SAP Cloud Application Programming Model (CAP)
SAP Extended Passport (EPP) Processing
SAP Integration Suite
SAP Manufacturing Integration and Intelligence
SAP NetWeaver (Message Server)
SAP NetWeaver (SAP GUI for Java)

SAP NetWeaver Business Client
SAP S/4HANA (Intercompany Matching and Reconciliation)
SAP Web Dispatcher, Internet Communication Manager and SAP Content Server

Disclaimer