Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0119

Kwetsbaarheden verholpen in SAP-producten

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 30-04-2025
Revisie: 1.0.3

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

Update Revisie 3

SAP heeft een update op de advisorie van eerder deze maand

Feiten

SAP heeft kwetsbaarheden verholpen in verschillende producten, waaronder SAP Financial Consolidation, SAP Landscape Transformation, SAP NetWeaver Application Server ABAP, SAP Commerce Cloud, SAP ERP BW, SAP BusinessObjects Business Intelligence Platform, SAP KMC WPC, SAP Solution Manager, SAP S4CORE, en SAP CRM.

Duiding

De uitgebrachte paches bevatten een aantal kritieke kwetsbaarheden met de kenmerken CVE-2025-30016, CVE-2025-31330 en CVE-2025-27429.

De kwetsbaarheid met kenmerk CVE-2025-30016 is een kritieke authenticatie-bypass in SAP Financial Consolidation, die ongeauthenticeerde aanvallers toegang geeft tot het Admin-account.

SAP Landscape Transformation heeft een kwetsbaarheid met kenmerk CVE-2025-31330, die het mogelijk maakt voor aanvallers met gebruikersprivileges om willekeurige ABAP-code in te voegen.

De kwetsbaarheid met kenmerk CVE-2025-27429 in SAP S/4HANA (Private Cloud) stelt een aanvaller met gebruikersprivileges in staat om willekeurige ABAP-code in de RFC-functiemodule te injecteren en autorisatiecontroles te omzeilen, waardoor de vertrouwelijkheid, integriteit en beschikbaarheid van het systeem in gevaar komen.

SAP NetWeaver Application Server ABAP heeft een Mixed Dynamic RFC Destination-kwetsbaarheid die kan leiden tot blootstelling van gevoelige inloggegevens. Daarnaast zijn er kwetsbaarheden in SAP Commerce Cloud die de vertrouwelijkheid en integriteit van gegevens in gevaar kunnen brengen. De kwetsbaarheden in SAP ERP BW en SAP BusinessObjects kunnen leiden tot ongeautoriseerde uitvoering van commando's en wijziging van bestanden. De directory traversal-kwetsbaarheden in SAP Capital Yield Tax Management en SAP Solution Manager stellen aanvallers in staat om gevoelige informatie te verkrijgen. De SSRF-kwetsbaarheid in SAP CRM en SAP S/4HANA kan de vertrouwelijkheid van interne netwerkbronnen in gevaar brengen.

UPDATE 25/04/2025 SAP heeft een update uitgebracht op de advisory van eerder deze maand. De belangrijkste aanpassing is de toevoeging van **CVE-2025-31324**. Dit is een kritieke kwetsbaarheid waarbij de Metadata Uploader geen correcte autorisatiecontrole toepast. Hierdoor kan een niet-geauthenticeerde aanvaller kwaadaardige uitvoerbare bestanden uploaden naar de server.

UPDATE 28/04/2025 Het NCSC ontvangt meldingen dat de kwetsbaarheid met kenmerk CVE-2025-31324 actief wordt misbruikt. De getroffen Metadata Uploader is onderdeel van Visual Composer. Dit product, bedoeld om

zonder het schrijven van programmacode user-interfaces te bouwen, wordt al sinds 2015 niet meer ondersteund. Het gebruik ervan om interfaces te bouwen wordt daarom afgeraden. Ook is het goed gebruik een dergelijk ontwerpsoftware niet publiek toegankelijk te hebben, maar te hosten in een separate ontwikkelomgeving. In het geval van Visual Composer kan de toegang worden beperkt door de applicatia-alias `developmentserver` uit te schakelen en middels firewall rules de toegang tot de development-server applicatie-url te blokkeren.

UPDATE 30/04/2025 In de eerdere update van dit beveiligingsadvies op 28/04/2025 heeft het NCSC gemeld dat de kwetsbaarheid met het kenmerk CVE-2025-31324 actief wordt misbruikt. Een onderdeel van het misbruik is dat kwaadwillenden webshells plaatsen. Na nader onderzoek door het NCSC en op basis van ontvangen meldingen, is ook waargenomen dat deze webshells online te koop wordt aangeboden. Dit vergroot de kans op misbruik aanzienlijk. Het NCSC heeft daarom besloten om dit beveiligingsadvies naar H/H te verhogen.

Oplossingen

SAP heeft patches uitgebracht om de kwetsbaarheden in de genoemde producten te verhelpen.

Ook heeft SAP voor de kwetsbaarheid met kenmerk CVE-2025-31324 een noodpatch uitgebracht om deze te verhelpen. Het NCSC adviseert om naast de reguliere updates vooral deze noodpatch ook in te zetten.

UPDATE 30/04/2025 Het NCSC adviseert met klem om de beschikbaar gestelde beveiligingsupdates te installeren en uw systeem op aanwezigheid van webshells te controleren. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html
- https://me.sap.com/notes/3594142
- https://reliaquest.com/blog/threat-spotlight-reliaquest-uncovers-vulnerability-behind-sap-netweaver-compromise/
- https://onapsis.com/blog/active-exploitation-of-sap-vulnerability-cve-2025-31324/

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-56337	7.2 HIGH
CVE-2025-0064	5.1 MEDIUM
CVE-2025-23186	8.5 HIGH

CVE-2025-26653	5.3 MEDIUM
CVE-2025-26654	6.3 MEDIUM
CVE-2025-26657	6.9 MEDIUM
CVE-2025-27428	5.3 MEDIUM
CVE-2025-27429	8.7 HIGH
CVE-2025-27430	3.5 LOW
CVE-2025-27435	2.3 LOW
CVE-2025-27437	4.3 MEDIUM
CVE-2025-30013	8.6 HIGH
CVE-2025-30014	5.3 MEDIUM
CVE-2025-30015	4.1 MEDIUM
CVE-2025-30016	9.3 CRITICAL
CVE-2025-30017	4.8 MEDIUM
CVE-2025-31324	10.0 CRITICAL
CVE-2025-31327	5.3 MEDIUM
CVE-2025-31328	5.3 MEDIUM
CVE-2025-31330	8.7 HIGH
CVE-2025-31331	4.3 MEDIUM
CVE-2025-31332	4.8 MEDIUM
CVE-2025-31333	5.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-35	Path Traversal: '.../...//'
CWE-277	Insecure Inherited Permissions
CWE-921	Storage of Sensitive Data in a Mechanism without Access Control
CWE-472	External Control of Assumed-Immutable Web Parameter
CWE-319	Cleartext Transmission of Sensitive Information
CWE-862	Missing Authorization
CWE-918	Server-Side Request Forgery (SSRF)
CWE-863	Incorrect Authorization
CWE-787	Out-of-bounds Write
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-352	Cross-Site Request Forgery (CSRF)

Getroffen producten

SAP
BusinessObjects Financial Consolidation
ERP Financials Information System
Enterprise Extension Financial Services

Enterprise Financial Services
Financial Consolidation
Financial Consolidation Cube Designer
NetWeaver
NetWeaver (SAP Enterprise Portal)
NetWeaver AS ABAP (BSP Framework)
NetWeaver AS ABAP (Business Server Pages application)
Commerce
Commerce Cloud
Landscape Management
Solution Manager
Commerce Data Hub
Business Application Software Integrated Solution
Landscape Transformation
Netweaver System Landscape Directory
landscape_management

ATOSS
ATOSS Staff Efficiency Suite
Amazon
Amazon Linux 2
Apache
Tomcat
tomcat
SAP_SE
SAP S/4HANA (Private Cloud)
SAP Landscape Transformation (Analysis Platform)
SAP NetWeaver AS Java (System Landscape Directory)
sap
landscape_management
landscape_transformation_replication_server

Disclaimer