THREAT INTELLIGENCE BRIEFING

CVE-2026-120017

Anmeldung als beliebiger Nutzer über SAP-SAML2-SSO.

Ein nicht authentifizierter Angreifer kann dem SAML2-Dienst eines SAP-ABAP-Systems manipulierte Anmeldedaten vorlegen und sich als beliebiger Nutzer anmelden – bis hin zu privilegierten Konten. SAP bewertet die Lücke mit dem Höchstwert 10,0 und hat sie am Patch Day 10.11.2026 mit SAP Note 3849308 geschlossen. Eine Ausnutzung ist bislang nicht bekannt; die Lücke gilt aber als automatisierbar.

> **Geschäftsrisiko:** vollständige Übernahme des SAP-Systems mit Zugriff auf Finanz-, Personal- und Kundendaten – mit Potenzial für Manipulation von Geschäftsprozessen, Betriebsunterbrechung und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

10,0 / 10

KRITISCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H` – aus dem Netz, ohne Rechte, ohne Zutun, mit vollständiger Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit – auch über das betroffene System hinaus. Höchstwert; von SAP als CNA vergeben, von NIST noch nicht eigenständig bewertet (NVD-Status „Received“).

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Keine Ausnutzung bekannt (Stand 10.11.2026)	SAP_BASIS 702 bis 922 mit SAML2-Anmeldung	Dringend – vor Ausnutzungsbeginn patchen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

10,0 · KRITISCH
CVSS-Schweregrad

Auth-Bypass
SAML2 Service Provider (SSO)

Nicht bekannt
Ausnutzung · nicht in CISA KEV · kein PoC öffentlich

Note 3849308
SAP Patch Day 10.11.2026

Die Ursache: Der SAML2 Service Provider in SAP NetWeaver AS ABAP prüft eingehende Anmelde-Assertions **unter bestimmten Konfigurationen nicht ausreichend** (CWE-347: fehlerhafte Prüfung einer kryptografischen Signatur). Ein Angreifer kann dadurch speziell präparierte Daten einreichen, die Authentifizierung umgehen und sich als beliebiger Nutzer ausgeben – einschließlich privilegierter Konten. Welche Konfigurationen genau betroffen sind, beschreibt SAP nur in der zugangsgeschützten Note.

ANGRIFFSKETTE

01	02	03	04
SSO erreichbar – SAML2-Anmeldung des ABAP-Systems ist aus dem Netz ansprechbar	**Assertion fälschen** – präparierte Anmeldedaten ohne gültige Prüfung einreichen	**Identität übernehmen** – Anmeldung als beliebiger Nutzer, auch privilegiert	**Systemübernahme** – voller Zugriff, Auswirkung auf angebundene Systeme möglich

Betroffenheit & Fixversionen

SAP_BASIS-Release	Verwundbar bis	Fixversion (Ziel)
702 · 731 · 740	SAP_BASIS 702, 731, 740	SAP Note 3849308
750 bis 758	SAP_BASIS 750–758	SAP Note 3849308
816	SAP_BASIS 816	SAP Note 3849308
920 · 921 · 922	SAP_BASIS 920, 921, 922	SAP Note 3849308

Betroffen sind laut SAP und NVD die SAML2-Service-Provider-Komponente der genannten SAP_BASIS-Releases – angreifbar **nur unter bestimmten Konfigurationen**, die SAP ausschließlich in der zugangsgeschützten Note beschreibt. Korrekturanleitung bzw. Support Package je Release der Note 3849308 im SAP for Me entnehmen. Einzelne Sekundärquellen nennen abweichend nur 702–920; maßgeblich ist die SAP-Liste bis 922.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf ein SAP-System mit personenbezogenen Daten kann eine meldepflichtige Verletzung darstellen – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

30.10.2026
CVE-Nummer reserviert

10.11.2026
SAP Patch Day · Note 3849308 · CVSS 10,0

10.11.2026
CISA-Einstufung: keine Ausnutzung, automatisierbar

Stand heute
Keine Ausnutzung bekannt · nicht in CISA KEV

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – Betroffenheit vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
SAML2-Systeme inventarisieren	SAP Note 3849308 einspielen	Anmelde-Logs auswerten

01 Betroffenheit feststellen

Alle ABAP-Systeme auf SAP_BASIS 702–922 erfassen, bei denen die SAML2-Anmeldung aktiv ist – typischerweise Fiori, SAP GUI for HTML und Web-Services mit Single Sign-on. SAML2-Konfiguration (Transaktion SAML2) je Mandant prüfen und gegen die in der Note beschriebenen Bedingungen abgleichen.

02 Exposition reduzieren (vor dem Patch)

Öffentlich ist kein Workaround von SAP dokumentiert – einen etwaigen Workaround-Abschnitt in Note 3849308 prüfen. Bis zum Patch die Erreichbarkeit der SAML2-Endpunkte aus dem Internet und aus nicht vertrauenswürdigen Netzsegmenten einschränken. Das ersetzt den Patch nicht.

03 Patchen

SAP Note 3849308 per SNOTE bzw. das in der Note genannte Support Package für das eigene SAP_BASIS-Release einspielen – priorisiert auf extern erreichbaren Systemen. Am selben Patch Day hat SAP weitere Lücken mit CVSS 10,0 im NetWeaver-Stack geschlossen (u. a. ICM, Web Dispatcher, Gateway); den Patch-Zyklus gemeinsam planen.

04 Kompromittierung ausschließen

Security Audit Log (SM20 / RSAU_READ_LOG) auf SAML-Anmeldungen an privilegierten Konten, Anmeldungen aus unerwarteten Quellen und ungewöhnliche Nutzer-/Rollenänderungen seit dem 10.11.2026 auswerten. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Angebundene Systeme bewerten

SAP weist ausdrücklich darauf hin, dass die Auswirkung über das betroffene System hinausreichen kann. Vertrauensbeziehungen (RFC-Destinationen, Trusted Systems, Schnittstellen-Nutzer) des betroffenen Systems in die Prüfung einbeziehen.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Keine – Stand 10.11.2026 keine Ausnutzung bekannt, kein öffentlicher PoC

AUSWERTUNGSQUELLEN

Security Audit Log SM20 / RSAU_READ_LOG
ICM-/HTTP-Logs der SAML2-Endpunkte

AUFFÄLLIGE MUSTER

SAML-Anmeldung an privilegierten Konten
Anmeldungen aus fremden Quell-IPs
neue Nutzer / Rollen kurz nach Login

Zur Einordnung: Es liegen keine CVE-spezifischen Indikatoren vor. Die genannten Muster sind Ansatzpunkte für eine Auswertung, keine bestätigten Signaturen – eine erfolgreiche Ausnutzung erscheint als reguläre SSO-Anmeldung.

Wichtig: Eine erfolgreiche Ausnutzung erscheint als ganz normale SSO-Anmeldung eines gültigen Nutzers – ohne Alarm. Ohne kontinuierliche Auswertung der SAP-Anmeldeprotokolle bleibt ein Zugriff unsichtbar.

Bildmotive: KI-generierte Symbolbilder

Lassen Sie das von unseren Experten prüfen.

Drei Bausteine, die genau auf diese Schwachstelle einzahlen – vom schnellen Exposure-Check bis zur laufenden Absicherung.

Cyber Defense Center

24/7-SOC aus München: Die SSO-Anmeldung an einem privilegierten SAP-Konto aus ungewöhnlicher Quelle fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden über SAML2 angebundene, ungepatchte SAP-ABAP-Systeme über Ihren gesamten Perimeter – bevor Angreifer sie finden – und priorisieren nach realer Ausnutzung.

Incident-Response-Retainer

Bei Verdacht auf einen bereits erfolgten Zugriff übernimmt unser IR-Team Forensik und Eindämmung – mit vertraglich zugesicherter Reaktionszeit.

SO GEHEN WIR VOR

01 Exposure-Check

Wir prüfen, ob Ihre SAP-Systeme verwundbar konfiguriert und exponiert sind.

02 Sofortmaßnahmen begleiten

Mitigation und Patch-Fahrplan gemeinsam mit Ihrem Team umgesetzt.

03 Absichern & überwachen

Threat Hunting auf die IoCs, danach laufendes Monitoring und IR-Bereitschaft – 24/7, wenn Ihr Team das nicht selbst leisten kann.

Empfehlung für die Geschäftsleitung

- Einspielen von SAP Note 3849308 priorisiert anordnen – extern erreichbare Systeme zuerst.
- Prüfen lassen, welche SAP-Systeme SAML2-Anmeldung nutzen und ob bereits auffällige Anmeldungen vorliegen.
- Über eine dauerhafte Überwachung der SAP-Anmeldeprotokolle entscheiden.

Ihr Part · unser Part. **Sie behalten die Kontrolle über Konfiguration und Freigaben; wir liefern Analyse, Bewertung und – im Retainer – die Reaktionskette.**

Rollen, Eingriffstiefe und SLAs im Erstgespräch (RACI, AVV/TOM auf Anfrage) · Datenhaltung auf Wunsch vollständig in Deutschland · ISO/IEC 27001 (TÜV SÜD) · deutschsprachige Analysten.

Sprechen Sie mit uns, bevor es ein Angreifer tut.

Kostenloses 30-Minuten-Erstgespräch – wir prüfen Ihre Exposure gegenüber CVE-2026-120017 und dem SAP-Perimeter.

+49 89 45 24 24-100 · kontakt@argos.security · www.argos.security

Termin buchen

Quellen: SAP Security Patch Day November 2026 (support.sap.com, Note 3849308, CVSS 10,0, Priorität Critical) · NVD CVE-2026-120017 (CNA SAP, CVSS 3.1 10,0, CWE-347; NVD-Status „Received“, keine eigene NIST-Bewertung) · CVE.org-Eintrag inkl. CISA-ADP-SSVC (Exploitation: none, Automatable: yes, Technical Impact: total) · CISA Known Exploited Vulnerabilities Catalog (Stand 10.11.2026: nicht gelistet). Ergänzend, Sekundärquellen: Rescana, RedRays, Bytelota. Angaben nach bestem Wissen zum Stand 10.11.2026; Korrekturanleitung und Konfigurationsbedingungen gegen SAP Note 3849308 abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.

Stand: 10.11.2026 · Argos Security · Cyber Defense Center

Bildmotive: KI-generierte Symbolbilder