THREAT INTELLIGENCE BRIEFING

CVE-2026-89103

Broken Access Control im SAP Gateway.

Das SAP Gateway – die zentrale Kommunikationskomponente jedes SAP-Applikationsservers für RFC-Verbindungen – aktiviert eine Standard-Zugriffsliste mit zu hohen Rechten. Ein externer Angreifer kann dadurch als interner Applikationsserver eingestuft werden und ohne Anmeldung unbefugte Aktionen in der SAP-Umgebung ausführen. SAP bewertet die Lücke mit dem Höchstwert 10,0; eine Ausnutzung ist bislang nicht bekannt.

> **Geschäftsrisiko:** unbefugte Aktionen im SAP-Kernsystem – mit Potenzial für Manipulation von Geschäftsdaten, Datenabfluss, Stillstand von Finanz-, Logistik- und Produktionsprozessen 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 Anmeldung, ohne Zutun eines Nutzers, mit Wirkung über das Gateway hinaus auf die gesamte Anwendungsumgebung. Höchstmöglicher Wert, vergeben von SAP als CNA; NVD hat noch keine eigene Bewertung vorgenommen.

AUSGENUTZT SEIT
Keine Ausnutzung bekannt (Stand 10.11.2026)

BETROFFEN
SAP-Kernel 7.22 – 9.21 (SAP Gateway)

HANDLUNGSBEDARF
Kurzfristig – mit nächstem Wartungsfenster, Exposition sofort prüfen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

10,0 · KRITISCH
CVSS-Schweregrad (SAP)

Ohne Anmeldung
Netzzugang zum SAP Gateway genügt

Nicht bekannt
Ausnutzung · nicht in CISA KEV · kein PoC

Kernel 7.22–9.21
SAP Note 3798345 · Patch Day 10.11.

Die Ursache: Laut SAP aktiviert das Gateway eine **Standard-Access-Control-List mit hohen Rechten**. Diese Liste entscheidet, welche Gegenstellen als vertrauenswürdige, interne Applikationsserver gelten. Durch die zu großzügige Voreinstellung kann ein **externer Angreifer als interner Applikationsserver** kategorisiert werden – und erhält damit Möglichkeiten, die eigentlich nur Systemen der eigenen SAP-Landschaft zustehen. SAP ordnet die Schwäche als fehlerhafte Autorisierung ein (CWE-863).

ANGRIFFSKETTE

01 **Gateway erreichbar** – Angreifer hat Netzzugang zum SAP Gateway

02 **Falsche Einstufung** – die Standard-ACL stuft ihn als internen Applikationsserver ein

03 **Vertrauen missbraucht** – ohne Anmeldung Zugriff auf Gateway-Funktionen der Landschaft

04 **Wirkung** – unbefugte Aktionen mit hohen Folgen für Vertraulichkeit, Integrität, Verfügbarkeit

Betroffenheit & Fixversionen

SAP-Kernel-Release	Verwundbar bis	Fixversion (Ziel)
7.22 / 7.22EXT	KERNEL · KRNL64UC · KRNL64NUC	SAP Note 3798345
7.53 / 7.54	KERNEL · KRNL64UC 7.53	SAP Note 3798345
7.77 / 7.93	KERNEL	SAP Note 3798345
8.04	KERNEL · KRNL64UC	SAP Note 3798345
9.16 / 9.20 / 9.21	KERNEL	SAP Note 3798345

Versionsangaben laut SAP-Patchday-Tabelle (10.11.2026); der CVE-Eintrag bei NVD/CVE.org führt dieselben Releases in verkürzter Form. Die konkreten Kernel-Patch-Stände stehen in der SAP Note 3798345 (Login im SAP for Me erforderlich) – **eigenen Kernel-Stand je System gegen die Note abgleichen**, auch für Standalone-Gateways.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf SAP-Systeme mit personenbezogenen oder geschäftskritischen 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

10.09.2026
CVE-Nummer reserviert
CVE-2026-89103 · Überblick

10.11.2026
SAP Security Patch Day · SAP Note 3798345

10.11.2026
CVE veröffentlicht · CVSS 10,0 (SAP)

Stand heute
Keine Ausnutzung bekannt · nicht in CISA KEV

Seite 3: Ihr Maßnahmenplan →

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
Gateway-Exposition prüfen und	SAP Note 3798345 einspielen	Gateway-Zugriffe überwachen

01 Betroffenheit feststellen

Alle SAP-Systeme mit Kernel 7.22 bis 9.21 inventarisieren – ABAP-Applikationsserver ebenso wie Standalone-Gateways. Kernel-Release und Patch-Stand je Instanz erfassen und gegen die SAP Note 3798345 abgleichen.

02 Exposition sofort einschränken

Prüfen, von wo das SAP Gateway erreichbar ist. Es darf weder aus dem Internet noch aus Nutzer- oder Gastnetzen zugänglich sein – nur aus den Netzen, in denen tatsächlich RFC-Partner stehen. Netzwerk-Freigaben und Firewall-Regeln entsprechend nachziehen. Diese Maßnahme reduziert das Risiko, ersetzt aber nicht den Patch.

03 Patchen

Die `SAP Note 3798345` einspielen – in der Regel über ein Kernel-Update auf den in der Note genannten Patch-Stand. Kernel-Updates erfordern einen Neustart der Instanz; Wartungsfenster entsprechend priorisieren, beginnend mit produktiven und von außen erreichbaren Systemen.

04 Gateway-Zugriffsregeln überprüfen

Die Gateway-Sicherheitsdateien (`reginfo`, `secinfo`) und die Gateway-Parameter Ihrer Systeme gegen die SAP-Härtungsempfehlungen prüfen lassen – zu weit gefasste Regeln sind ein bekanntes Risiko, unabhängig von dieser CVE. Ob die Note zusätzliche Konfigurationsschritte vorsieht, ergibt sich aus der Note selbst.

05 Kompromittierung ausschließen

Gateway-Logs und registrierte RFC-Programme (Transaktion `SMGW`) auf Verbindungen von unbekannten Hosts und unerwartete Programmregistrierungen prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

WO HINSCHAUEN

Gateway-Log und -Monitor
`SMGW` · Security Audit Log
`SM20` / `RSAU_READ_LOG`

AUFFÄLLIGE MUSTER

Gateway-Verbindungen von Hosts außerhalb der SAP-Landschaft
unerwartete registrierte RFC-Programme

VERÖFFENTLICHTE IOCS

Keine (Stand 10.11.2026)
keine bekannte Ausnutzung
kein öffentlicher PoC

Zur Einordnung: Für diese Schwachstelle sind keine Indikatoren veröffentlicht. Die genannten Prüfpunkte sind allgemeine Anhaltspunkte für unbefugte Gateway-Zugriffe, keine CVE-spezifischen Signaturen. Erscheinen technische Details oder ein Exploit, ändert sich die Lage schnell – SAP-Lücken dieser Klasse werden erfahrungsgemäß zügig nachgebaut.

Wichtig: Das SAP Gateway läuft auf jedem ABAP-Applikationsserver mit – es ist kein optionales Zusatzprodukt. Weil die Schwäche in einer Standardeinstellung liegt, kann jedes System mit betroffenem Kernel angreifbar sein, sofern das Gateway aus dem Netz des Angreifers erreichbar ist. Dass heute keine Ausnutzung bekannt ist, ist kein Grund, den Patch aufzuschieben.

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: Gateway-Verbindungen und RFC-Registrierungen von Hosts außerhalb der SAP-Landschaft fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden aus fremden Netzen erreichbare, ungepatchte SAP Gateways 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

- Heute anordnen: Erreichbarkeit aller SAP Gateways prüfen und auf die notwendigen Netze beschränken.
- SAP Note 3798345 im nächsten Wartungsfenster einspielen lassen – produktive und exponierte Systeme zuerst.
- Über eine dauerhafte Überwachung der SAP-Landschaft entscheiden, damit unbefugte Zugriffe nicht unbemerkt bleiben.

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-2026-89103 und dem SAP-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen (primär): SAP Security Patch Day – November 2026 (support.sap.com, 10.11.2026, Note 3798345, Priorität Critical, CVSS 10,0) · NVD-Eintrag CVE-2026-89103 (Status „Received“, CVSS 3.1 10,0 von SAP als CNA, CWE-863, Referenz me.sap.com/notes/3798345) · CVE.org-Record CVE-2026-89103. Sekundärquellen (Onapsis, SecurityBridge, Pathlock) lagen zum Stand 10.11.2026 noch nicht vor und wurden nicht verwendet. Stand 10.11.2026: nicht im CISA-KEV-Katalog, keine Ausnutzung und kein öffentlicher PoC bekannt. Kernel-Patch-Stände gegen die SAP Note 3798345 abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.