THREAT INTELLIGENCE BRIEFING

CVE-2026-76964

Speicherkorruption im ICM von SAP NetWeaver AS ABAP.

Ein nicht angemeldeter Angreifer kann mit präpariertem Netzwerkverkehr eine Speicherkorruption im Internet Communication Manager (ICM) von SAP NetWeaver AS ABAP auslösen und damit beliebigen Code ausführen – bis zur vollständigen Übernahme des SAP-Systems. Der ICM nimmt die HTTP(S)-Verbindungen des ABAP-Systems entgegen. SAP hat am Patch Day 10.11.2026 die Security Note 3778530 veröffentlicht; eine Ausnutzung ist bislang nicht bekannt.

> **Geschäftsrisiko:** Übernahme zentraler ERP-Systeme – mit Potenzial für Datenabfluss, Manipulation von Geschäftsprozessen und Buchungen, 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 Anmeldung, ohne Zutun eines Nutzers, mit Wirkung über das ABAP-System hinaus. Höchstwert der Skala; von SAP als CNA vergeben, NVD-Prüfung noch ausstehend.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Keine Ausnutzung bekannt (Stand 10.11.2026)	SAP Kernel 7.53–9.20 ICM von AS ABAP	Vorrangig – vor der ersten Ausnutzung

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

10,0 · KRITISCH
CVSS-Schweregrad (SAP)

Pre-Auth-RCE
Speicherkorruption im ICM (CWE-1287)

Nicht bekannt
Ausnutzung · kein KEV · kein öffentlicher PoC

Note 3778530
SAP Patch Day 10.11.2026

Die Ursache: SAP NetWeaver AS ABAP prüft bestimmte Netzwerkeingaben, die eine interne Komponente des **Internet Communication Manager** verarbeitet, nicht ausreichend (CWE-1287, unzureichende Prüfung des Eingabetyps). Mit gezielt präpariertem Netzwerkverkehr lässt sich eine **Speicherkorruption** auslösen. Gelingt die Ausnutzung, kann der Angreifer **ohne Anmeldung beliebigen Code** ausführen und das System vollständig kompromittieren. Technische Details hat SAP nur in der zugangsgeschützten Note veröffentlicht.

ANGRIFFSKETTE

01	02	03	04
ICM erreichbar – HTTP(S)-Dienst des ABAP-Systems aus dem Netz, ggf. über Web Dispatcher veröffentlicht	**Präparierter Verkehr** – manipulierte Netzwerkeingabe an die betroffene interne Komponente	**Speicherkorruption** – im ICM-Prozess, vor jeder Anmeldung	**Codeausführung** – volle Kontrolle über das SAP-System und seine Daten

Betroffenheit & Fixversionen

Komponente	Verwundbar bis	Fixversion (Ziel)
SAP Kernel (KERNEL)	7.53 · 7.54 · 7.77 · 7.93 · 9.16 · 9.18 · 9.20	SAP Note 3778530 einspielen
SAP Kernel Unicode (KRNL64UC)	7.53	SAP Note 3778530 einspielen

Versionsangaben laut SAP-Patchday-Tabelle und CVE-Eintrag (Produkt „SAP NetWeaver AS ABAP (Internet Communication Manager)“). Die konkreten Kernel-Patch-Level stehen nur in der Note 3778530 im SAP-Support-Portal – Anmeldung erforderlich. Am selben Patch Day: Note 3778556 (CVE-2026-89126, CVSS 10,0) für den **SAP Web Dispatcher** – Kernel-Updates gemeinsam planen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf SAP-Systeme 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

20.08.2026
CVE-Nummer reserviert

10.11.2026
SAP Patch Day · Note 3778530 · CVSS 10,0

10.11.2026
NVD-Eintrag veröffentlicht (Status „Received“)

Stand heute
Kein KEV-Eintrag · kein öffentlicher PoC bekannt

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – Inventar vor Patch, Exposition reduzieren, bevor Exploits erscheinen.

SOFORT	KURZFRISTIG	PARALLEL
ABAP-Systeme inventarisieren, ICM-Exposition prüfen	Note 3778530 einspielen	Überwachung der ICM-Prozesse

01 Betroffenheit feststellen

Alle AS-ABAP-Systeme erfassen und Kernel-Release sowie Patch-Level je System mit der Versionsliste der Note abgleichen (z. B. über `disp+work -v` oder Transaktion `SM51` → Release-Info).

02 Exposition reduzieren

Prüfen, welche ICM-Ports (HTTP/HTTPS, Transaktion `SMICM`) aus dem Internet oder aus wenig vertrauenswürdigen Netzen erreichbar sind. Bis zum Patch den Zugriff auf das Nötige beschränken – das senkt das Risiko, schließt eine Speicherkorruption aber nicht.

03 Patchen

SAP Note `3778530` im SAP-Support-Portal aufrufen und den dort genannten Kernel-Patch einspielen. Exponierte Systeme zuerst. Eventuell in der Note beschriebene Behelfslösungen nur als Übergang nutzen.

04 Web Dispatcher mitpatchen

Am selben Patch Day hat SAP mit Note `3778556` eine weitere Speicherkorruption (CVSS 10,0) im SAP Web Dispatcher behoben – bei Kernel-Updates beide Notes in einem Wartungsfenster bündeln.

05 Auffälligkeiten überwachen

Abstürze und Neustarts des ICM, Core Dumps sowie ungewöhnliche Prozesse oder ausgehende Verbindungen der Applikationsserver als Alarm behandeln. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

PROZESS-AUFFÄLLIGKEITEN

Abstürze / Neustarts des ICM (`icman`), Core Dumps, Einträge in `dev_icm`

HOST-AUFFÄLLIGKEITEN

neue Kindprozesse des SAP-Kernels, z. B. `sh` · `bash` · `curl` · `wget`

NETZWERK

ungewöhnliche ausgehende Verbindungen der SAP-Applikationsserver

Zur Einordnung: Zum Stand 10.11.2026 sind keine kampagnenbezogenen IoCs veröffentlicht – es ist keine Ausnutzung bekannt. Die genannten Punkte sind generische Hinweise für eine Speicherkorruption mit Codeausführung, keine bestätigten Angriffsmerkmale.

Wichtig: Erfahrungsgemäß folgen bei kritischen SAP-Lücken Patch-Analysen und Exploits oft innerhalb weniger Tage. Ein Angriff auf den ICM erfolgt vor jeder Anmeldung – klassische Berechtigungskontrollen im SAP-System greifen nicht. Das Zeitfenster für einen ruhigen Patch ist jetzt.

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: Abstürze des ICM-Prozesses und ungewöhnliche Prozessstarts auf den SAP-Applikationsservern fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden aus dem Internet erreichbare, 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

- Patch der Note 3778530 vorrangig anordnen – exponierte Systeme zuerst, idealerweise innerhalb weniger Tage.
- Inventar aller SAP-ABAP-Systeme, ihrer Kernel-Stände und ihrer Erreichbarkeit aus dem Internet einfordern.
- Über eine dauerhafte Überwachung der SAP-Landschaft und ihres Perimeters 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-2026-76964 und dem SAP-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: SAP Security Patch Day – November 2026 (support.sap.com, Note 3778530, Priorität Critical, CVSS 10,0, Versionen KRNL64UC 7.53, KERNEL 7.53–9.20) · NVD-Eintrag CVE-2026-76964 (Status „Received“, CVSS 3.1 von SAP als CNA, CWE-1287, Referenz me.sap.com/notes/3778530) · CVE.org-Eintrag (veröffentlicht 10.11.2026) · CISA Known Exploited Vulnerabilities Catalog (Version 2026.11.10, kein Eintrag). Sekundärquellen, ergänzend: Rescana und rz10.de (Patchday-Analysen, keine Ausnutzung/kein PoC genannt). Angaben nach bestem Wissen zum Stand 10.11.2026; Kernel-Patch-Level gegen SAP Note 3778530 abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.