THREAT INTELLIGENCE BRIEFING

CVE-2026-89126

Speicherkorruption im SAP Web Dispatcher.

Ein nicht angemeldeter Angreifer kann mit präpariertem Netzwerkverkehr einen Heap-Überlauf im SAP Web Dispatcher auslösen und damit beliebigen Code ausführen – bis zur vollständigen Übernahme des Systems. Der Web Dispatcher steht häufig als Eingangstor direkt vor der SAP-Landschaft und ist aus dem Internet erreichbar. SAP hat am Patch Day 10.11.2026 die Security Note 3778556 veröffentlicht; eine Ausnutzung ist bislang nicht bekannt.

> **Geschäftsrisiko:** Übernahme des Eingangstors zur SAP-Landschaft – mit Potenzial für Datenabfluss aus ERP-Systemen, 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 Anmeldung, ohne Zutun eines Nutzers, mit Wirkung über das Web-Dispatcher-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)	Web Dispatcher 7.53–9.20 + HANA / XS Advanced	Vorrangig – vor der ersten Ausnutzung

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

10,0 · KRITISCH
CVSS-Schweregrad (SAP)

Pre-Auth-RCE
Heap-Überlauf (CWE-122)

Nicht bekannt
Ausnutzung · kein KEV · kein öffentlicher PoC

Note 3778556
SAP Patch Day 10.11.2026

Die Ursache: Der SAP Web Dispatcher prüft bestimmte Netzwerkeingaben, die eine interne Komponente verarbeitet, nicht ausreichend. Mit gezielt präpariertem Netzwerkverkehr lässt sich ein **Heap-basierter Pufferüberlauf** (CWE-122) 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
Web Dispatcher erreichbar – als Reverse Proxy / Load Balancer vor SAP-Systemen, oft aus dem Internet	**Präparierter Verkehr** – manipulierte Netzwerkeingabe an die betroffene interne Komponente	**Speicherkorruption** – Heap-Überlauf im Web-Dispatcher-Prozess	**Codeausführung** – volle Kontrolle über das System, Sprungbrett in die SAP-Landschaft

Betroffenheit & Fixversionen

Komponente	Verwundbar bis	Fixversion (Ziel)
SAP Web Dispatcher (WEBDISP)	7.53	SAP Note 3778556 einspielen
SAP Kernel (KERNEL / KRNL64UC)	7.53 · 7.54 · 7.77 · 7.93 · 9.16 · 9.18 · 9.20	SAP Note 3778556 einspielen
SAP HANA (HDB)	2.00	SAP Note 3778556 einspielen
XS Advanced Runtime	1.00	SAP Note 3778556 einspielen
SAP Extended App Services	1	SAP Note 3778556 einspielen

Versionsangaben laut SAP-Patchday-Tabelle und CVE-Eintrag. Die konkreten Patch-Level (Web-Dispatcher- bzw. Kernel-Patch) stehen nur in der Note 3778556 im SAP-Support-Portal – Anmeldung erforderlich. Auch **eingebettete Web Dispatcher** in HANA und XS Advanced prüfen. Am selben Patch Day: Note 3778530 (CVE-2026-76964, CVSS 10,0) für den ICM des AS ABAP – gemeinsam bewerten.

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

10.09.2026
CVE-Nummer reserviert

10.11.2026

10.11.2026

Seite 3: Ihr Maßnahmenplan → Stand heute

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
Web Dispatcher inventarisieren, Exposition prüfen	Note 3778556 einspielen	Überwachung der Web-Dispatcher-Instanzen

01 Betroffenheit feststellen

Alle Web-Dispatcher-Instanzen erfassen – eigenständig, im Kernel und eingebettet in HANA / XS Advanced. Version und Patch-Level je Instanz mit der Versionsliste der Note abgleichen (z. B. über `sapwebdisp -v` bzw. die Web-Administrationsoberfläche).

02 Exposition reduzieren

Prüfen, welche Instanzen aus dem Internet oder aus wenig vertrauenswürdigen Netzen erreichbar sind. Bis zum Patch den Zugriff auf das Nötige beschränken – Administrationsoberfläche und nicht benötigte Ports nicht öffentlich anbieten.

03 Patchen

SAP Note 3778556 im SAP-Support-Portal aufrufen und den dort genannten Web-Dispatcher- bzw. Kernel-Patch einspielen. Exponierte Instanzen zuerst. Eventuell in der Note beschriebene Behelfslösungen nur als Übergang nutzen.

04 Gleichzeitig ICM patchen

Am selben Patch Day hat SAP mit Note 3778530 eine weitere Speicherkorruption (CVSS 10,0) im ICM des AS ABAP behoben – bei Kernel-Updates beide Notes in einem Wartungsfenster bündeln.

05 Auffälligkeiten überwachen

Abstürze, unerwartete Neustarts und Core Dumps des Web-Dispatcher-Prozesses sowie ungewöhnliche Prozesse oder ausgehende Verbindungen des Web-Dispatcher-Hosts als Alarm behandeln. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

PROZESS-AUFFÄLLIGKEITEN

Abstürze / Neustarts von `sapwebdisp`, Core Dumps

HOST-AUFFÄLLIGKEITEN

neue Kindprozesse des Web Dispatchers, z. B. `sh` · `bash` · `curl` · `wget`

NETZWERK

ungewöhnliche ausgehende Verbindungen des Web-Dispatcher-Hosts

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: CISA stuft die Ausnutzung als automatisierbar ein. Erfahrungsgemäß folgen bei kritischen SAP-Lücken Analysen der Patches und Exploits oft innerhalb weniger Tage – 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 Web-Dispatcher-Prozesses und ungewöhnliche Prozessstarts auf dem Web-Dispatcher-Host 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 Web Dispatcher 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 3778556 vorrangig anordnen – exponierte Web Dispatcher zuerst, idealerweise innerhalb weniger Tage.
- Inventar aller Web-Dispatcher-Instanzen 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-2026-89126 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 3778556, Priorität Critical, CVSS 10,0) · NVD-Eintrag CVE-2026-89126 (Status „Received“, CVSS 3.1 von SAP als CNA, CWE-122, Referenz me.sap.com/notes/3778556) · CVE.org-Eintrag inkl. CISA-ADP-Einschätzung (Exploitation: none, Automatable: yes, Technical Impact: total). Sekundärquellen lagen zum Stand nicht vor. Angaben nach bestem Wissen zum Stand 10.11.2026; Patch-Level gegen SAP Note 3778556 abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.