AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-10520

Ivanti Sentry: unauthentifizierte Root-Übernahme über OS-Command-Injection.

Eine OS-Command-Injection in Ivanti Standalone Sentry erlaubt einem entfernten, nicht authentifizierten Angreifer Remote Code Execution mit Root-Rechten. Der verwundbare Endpunkt akzeptiert ein Konfigurations-Kommando ohne Anmeldung direkt aus dem Netz. Die Lücke ist mit CVSS 10,0 maximal bewertet, wird seit dem 11. Juni 2026 aktiv ausgenutzt und steht im CISA-KEV-Katalog.

> **Geschäftsrisiko:** Ein erfolgreicher Angriff bedeutet die vollständige Übernahme des Sentry-Gateways mit Root-Rechten. Damit steht dem Angreifer das zentrale Zugangs-Gateway zu Mobilgeräten und internen Diensten offen, inklusive Datenabfluss, Manipulation und Ausbreitung ins interne Netz.

10,0 / 10

KRITISCH
CVSS 3.1 BASISWERT

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H` – Über das Netzwerk, ohne Anmeldung und ohne Nutzerinteraktion aus der Ferne ausnutzbar; volle Kompromittierung von Vertraulichkeit, Integrität und Verfügbarkeit mit Ausbruch aus dem Sicherheitskontext.

AUSGENUTZT SEIT
11. Juni 2026

BETROFFEN
Betroffen ist **Ivanti Standalone Sentry** in allen Zweigen vor den Fix-Versionen.
Verwundbar: bis 10.5.1, 10.6.0–10.6.1 sowie 10.7.0.

HANDLUNGSBEDARF
Sofortmaßnahme – aktiv ausgenutzt, CVSS 10,0

Das Wichtigste in 60 Sekunden.

10,0	KEV	Root	3
CVSS-Score	aktiv ausgenutzt	Rechte bei RCE	Fix-Versionen

Die Ursache: Ursache ist eine unzureichende Filterung von Sonderzeichen bei einem OS-Kommando (CWE-78). Der Endpunkt `/mics/api/v2/sentry/mics-config/handleMessage` ist für interne Konfigurationskommandos gedacht, verarbeitet den `message`-Parameter aber ungeprüft und ohne Authentifizierung. So lässt sich beliebiger Betriebssystembefehl mit Root-Rechten einschleusen.

ANGRIFFSKETTE

01	02	03	04
Erreichen des exponierten Sentry-Endpunkts über das Netz, ohne Anmeldung.	**Einschleusen** eines präparierten `message`-Parameters mit OS-Kommando.	**Ausführung** des Befehls mit Root-Rechten (RCE) auf dem Gateway.	**Persistenz & Ausbreitung** ins interne Netz, Datenabfluss, Manipulation.

Betroffenheit & Fixversionen

Fix-Version	Verwundbar bis	Fixversion (Ziel)
Sentry 10.5.x	< 10.5.2	10.5.2
Sentry 10.6.x	< 10.6.2	10.6.2
Sentry 10.7.x	10.7.0	10.7.1

Verwundbar sind Versionen bis einschließlich 10.5.1, 10.6.1 und 10.7.0. Die Fixes 10.5.2, 10.6.2 und 10.7.1 sind laut Ivanti-Advisory und NVD-Beschreibung die abschließend behebenden Versionen; ein wirksamer Workaround wird nicht genannt.

Regulatorischer Hinweis: NIS-2: kritische, aktiv ausgenutzte Schwachstelle im Zugangs-Gateway – bei erfolgreicher Kompromittierung greifen Melde- und Reaktionspflichten (24/72 Stunden). DSGVO Art. 33/34: Bei Datenabfluss über das Gateway ist eine Meldung an Aufsichtsbehörde und ggf. Betroffene zu prüfen.

ZEITACHSE

09.06.2026
Ivanti veröffentlicht Security-Advisory und Patches

10.06.2026
Öffentlicher PoC (watchTowr); breite Ausnutzungsversuche (Shadowserver)

11.06.2026
Aufnahme in CISA-KEV – aktive Ausnutzung bestätigt

14.07.2026
Argos-Advisory: Patchstand prüfen, Kompromittierung ausschließen

Ihr Maßnahmenplan.

Vom Betroffenheits-Check bis zum Kompromittierungs-Ausschluss

SOFORT	≤ 24 H	≤ 72 H
Exposition prüfen, Zugriff auf Sentry aus dem Internet einschränken	Auf Fix-Version patchen (10.5.2 / 10.6.2 / 10.7.1)	Forensische Prüfung auf Kompromittierung, Reaktion einleiten

01 Betroffenheit feststellen

Alle Standalone-Sentry-Instanzen inventarisieren und Versionsstand prüfen. Verwundbar sind bis 10.5.1, 10.6.1 und 10.7.0.

02 Exposition reduzieren

Netzwerkzugriff auf das Sentry-Management/den API-Endpunkt aus dem Internet umgehend einschränken, bis der Patch aktiv ist.

03 Patchen

Auf die zum Zweig passende Fix-Version aktualisieren: 10.5.2, 10.6.2 oder 10.7.1.

```
# Zielversion je Zweig: 10.5.2 / 10.6.2
/ 10.7.1
```

04 Kompromittierung ausschließen

Aufgrund aktiver Ausnutzung: Logs des Endpunkts, unbekannte Root-Prozesse, neue Konten, Persistenz und ausgehende Verbindungen prüfen. Bei Verdacht IR auslösen.

05 Nachhärten

Management-Interfaces dauerhaft vom Internet trennen, Segmentierung und Monitoring des Gateways etablieren.

⚠ **Wichtig:** Reines Patchen genügt nicht: Da die Lücke seit dem 11. Juni 2026 aktiv ausgenutzt wird und ein öffentlicher PoC existiert, muss jede zuvor exponierte Instanz als potenziell kompromittiert behandelt und forensisch geprüft werden.

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: Auffällig im SOC/CDC: POST-Zugriffe auf /mics/api/v2/sentry/mics-config/handleMessage, unerwartete Root-Prozesse oder Shell-Aufrufe des Sentry-Dienstkontos, sowie neue ausgehende Verbindungen vom Gateway. fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte Standalone Sentry (aus dem Internet erreichbar) 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 Ivanti-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

- Sofort auf Fix-Versionen 10.5.2 / 10.6.2 / 10.7.1 patchen und Internet-Exposition schließen.
- Jede zuvor erreichbare Instanz forensisch auf Kompromittierung prüfen – aktive Ausnutzung ist bestätigt.
- Melde-/Reaktionspflichten (NIS-2, DSGVO) vorsorglich bewerten und dokumentieren.

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-2026-10520 und dem Ivanti-Perimeter.

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

Termin buchen

Stand: 14.07.2026 · Argos Security · Cyber Defense Center

NVD (CVE-2026-10520), Ivanti Security Advisory (hub.ivanti.com), CISA KEV, Rapid7, eSentire, Help Net Security, watchTowr Labs