AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-111357

Root-Rechteausweitung in Ivanti Connect Secure: letztes Glied der Zero-Day-Kette geschlossen.

Über einen Dienst, der Wartungsaufgaben als Root ausführt, können Angreifer auf Ivanti Connect Secure volle Root-Rechte erlangen. Die Lücke war das bisher ungepatchte Glied der im Oktober ausgenutzten Zero-Day-Kette um CVE-2026-104935; Ivanti hat am 29. Oktober 2026 Fixversionen veröffentlicht, CISA hat sie am 30. Oktober in den KEV-Katalog aufgenommen – mit Frist 2. November und forensischer Triage-Pflicht.

Geschäftsrisiko: Vollständige Übernahme des zentralen Fernzugangs bis auf Root-Ebene – mit Mitschnitt von VPN-Sitzungen, Zugriff auf Zugangsdaten und Verzeichnisdienst-Konten und schwer erkennbarer Persistenz; ein meldepflichtiger Sicherheitsvorfall nach NIS-2 / DSGVO ist dann wahrscheinlich.

7,0 / 10

HOCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | **Hoch** | Kritisch

`CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H` – lokal auf dem Gateway, mit erhöhtem Aufwand und einfachen Rechten; volle Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Basiswert der CNA MITRE, vom NVD übernommen; Fachmedien nennen unter Berufung auf Ivanti 8,8. Allein wirkt die Lücke nur lokal – in der Kette mit CVE-2026-104935 führt sie ohne Anmeldung bis Root.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
spätestens 03.10.2026	ICS 25.1.x bis 25.1.1.2 · 22.8R2 bis 22.8R2.5 Fix: 25.1.1.3 · 22.8R2.6	Sofort

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

7,0 · HOCH
CVSS 3.1 (MITRE · NVD)

Root
Rechteausweitung · CWE-829

Aktiv
ausgenutzt · CISA KEV · Frist 02.11.2026

Patch da
seit 29.10.2026 · kein Workaround

Die Ursache: Der privilegierte Hintergrunddienst **dsinvoked** führt Wartungsaufgaben auf Anforderung als Root aus und liest dafür aus dem gemeinsamen Konfigurationsspeicher **DSCache**, welches Programm er starten soll – ohne diesen Daten ausreichend zu misstrauen (**CWE-829**). Laut Volexity veränderten die Angreifer im Arbeitsspeicher eine Programmbibliothek, bogen einen Eintrag auf ein eigenes Skript um und erhielten so **Root-Rechte**. Danach stellten sie Eintrag und Bibliothek wieder her – das Prüfwerkzeug des Herstellers fand nichts.

ANGRIFFSKETTE

01 **Anmeldung umgangen** – CVE-2026-104935 über gefälschten Header

02 **Code ausgeführt** – hochgeladene Datei läuft im Webprozess

03 **Root erlangt** – DSCache-Eintrag lässt dsinvoked eigenes Skript starten

04 **Spuren verwischt** – Eintrag zurückgesetzt, Mitschnitt, Zugangsdaten

Betroffenheit & Fixversionen

Produkt / Zweig	Verwundbar bis	Fixversion (Ziel)
ICS 25.1.x	≤ 25.1.1.2	25.1.1.3
ICS 22.8R2	22.8R2 – 22.8R2.5	22.8R2.6
ICS 25.1.2.x / 25.1.3.x	laut Volexity betroffen	neuestes Release, s. Advisory

Fixstände **25.1.1.3 · 22.8R2.6** laut Ivanti-Advisory (Ergänzung vom 29.10.2026, wiedergegeben in der Fachpresse); die NVD-Auswertung deckt sich damit. Für die Zweige 25.1.2 und 25.1.3 nennt Volexity ebenfalls Handlungsbedarf – Stand bitte direkt im Hersteller-Advisory prüfen. Ein Workaround existiert nicht.

Regulatorischer Hinweis: Ein kompromittiertes VPN-Gateway ist in der Regel ein meldepflichtiger Sicherheitsvorfall – NIS-2 nach den für Sie geltenden Fristen, DSGVO bei personenbezogenen Daten unverzüglich (i. d. R. 72 h). Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung, Forensik und Dokumentation.

ZEITACHSE

03.10.2026
Erste Ausnutzung der Kette

13.10.2026
Volexity-Analyse · Fix für 104935

29.10.2026
Ivanti-Fix für die Root-Lücke

30.10.2026
CISA-KEV · Frist 02.11.2026

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – Version prüfen, sofort patchen, Kompromittierung forensisch ausschließen.

SOFORT	KURZFRISTIG	PARALLEL
Auf 25.1.1.3 bzw. 22.8R2.6	Dateisystem und Logs prüfen	Kompromittierung ausschließen

01 Betroffenheit feststellen

ICS-Version aller Gateways erheben und mit der Fixtabelle abgleichen. Auch wer im Oktober für CVE-2026-104935 gepatcht hat, ist hier noch verwundbar.

02 Patchen

Auf `25.1.1.3` bzw. `22.8R2.6` aktualisieren, vorher Konfiguration sichern. Einen Workaround gibt es nicht.

03 Spuren suchen

Nach Dateien wie `ics-root-run-inband-*.pl` und `/data/.icscap/` suchen; Lücken in Debug- und Audit-Log werten wie ein Treffer.

04 Kompromittierung ausschließen

Der Integrity Checker übersieht diese Angriffe. Bei Verdacht Speicher- und Netzwerkforensik, CISA verlangt eine forensische Triage.

Kompromittierungs-Indikatoren (IoCs)

ROOT-ARTEFAKTE

`/home/runtime/tmp/`
`ics-root-run-inband-*.pl`
`ics-root-result-inband-*`

PERSISTENZ & MITSCHNITT

`/data/.icscap/h.py` · `cap*`
`/data/.icscap/dsstatmond`
(umbenanntes tcpdump)

NETZWERK & LOGS

`108.165.147[.]64`
Manipulation an `debuglog` und `audit.log`

Zur Einordnung: Die Indikatoren stammen aus der Analyse von Volexity (13.10.2026, ergänzt 29.10.2026), nicht aus dem Hersteller-Advisory. Die IP-Adresse ist eine flüchtige Momentaufnahme; belastbarer sind Artefakte im Dateisystem und Lücken in den Logs.

Wichtig: Der Integrity Checker hat diese Angriffe nicht erkannt – die Angreifer patchen Code im Arbeitsspeicher und setzen ihre Änderungen zurück. Ein grünes Prüfergebnis ist hier keine Entwarnung.

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: Anfragen an die ICS-Anmeldeseite mit untypischen X-DSCGI-PATH-Headern, unerwartete Skripte unter /home/runtime/tmp sowie ausgehende Verbindungen vom VPN-Gateway ins interne Netz fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden Ivanti-Connect-Secure-Gateways vor 25.1.1.3 bzw. 22.8R2.6 – insbesondere solche, die vor dem Oktober-Patch aus dem Internet erreichbar waren 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

- Heute anordnen: alle Ivanti-Connect-Secure-Gateways auf 25.1.1.3 bzw. 22.8R2.6 bringen und den Abschluss bestätigen lassen.
- Für Gateways, die im Oktober erreichbar waren, eine forensische Prüfung beauftragen – das Prüftool des Herstellers reicht hier nicht.
- Bei Verdacht die über das Gateway genutzten Dienstkonten und Zugangsdaten erneuern – dokumentiert für eine etwaige Meldung.

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-2026-111357 und dem Ivanti-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Ivanti Security Advisory CVE-2026-104935 (ergänzt 29.10.2026) · CVE-Record CVE-2026-111357 (MITRE als CNA) · NVD CVE-2026-111357 · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 30.10.2026) · Volexity, Analyse der Angriffskette (13.10.2026, Update 29.10.2026). Angaben nach bestem Wissen zum Stand 02.11.2026 – gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.