

PREPARE PROTECT DETECT RESPOND IMPROVE

● AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-104935

Auth-Bypass in Ivanti Connect Secure: Befehlsausführung ohne Anmeldung am VPN-Gateway.

Über einen gefälschten Header können Angreifer die Anmeldung an Ivanti Connect Secure umgehen und ohne Zugangsdaten Befehle auf dem VPN-Gateway ausführen. Ivanti hat die Lücke am 13. Oktober 2026 mit Fixversionen veröffentlicht und bestätigt begrenzte Ausnutzung; CISA hat sie am selben Tag in den KEV-Katalog aufgenommen – mit forensischer Triage-Pflicht. Eine in derselben Kette genutzte Rechteauserweiterung ist noch nicht behoben.

Geschäftsrisiko: Übernahme des zentralen Fernzugangs – mit Zugriff auf VPN-Sitzungen, Zugangsdaten und Verzeichnisdienst-Konten, als Sprungbrett ins interne Netz; ein meldepflichtiger Sicherheitsvorfall nach NIS-2 / DSGVO ist dann wahrscheinlich.

8,6 / 10

HOCH

CVSS 3.1 BASISWERT



CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L – aus dem Netz, mit geringem Aufwand, ohne Anmeldung und ohne Zutun eines Nutzers; hohe Wirkung auf die Vertraulichkeit. Basiswert von Ivanti als CNA, vom NVD übernommen. In der beobachteten Angriffskette wird die Lücke mit einer weiteren, noch ungepatchten Rechteauserweiterung bis Root kombiniert.

AUSGENUTZT SEIT

spätestens 03.10.2026

BETROFFEN

ICS 22.8R2 – 22.8R2.4 · 25.1.x vor 25.1.3.0
Fix: 25.1.3.0 · 25.1.3.1 · 22.8R2.5

HANDLUNGSBEDARF

Sofort

Das Wichtigste in 60 Sekunden.

8,6 · HOCH

CVSS 3.1 (Ivanti · NVD)

Auth-Bypass

Spoofing · ohne Anmeldung · CWE-290

Aktiv

ausgenutzt · CISA KEV · Frist 16.10.2026

Patch da

Root-Rechteausweitung noch offen



Die Ursache: Connect Secure vertraut beim Weiterleiten von Anfragen einem vom Client gesetzten Header: Über die öffentlich erreichbare Anmeldeseite lassen sich so auch **geschützte interne Programme** aufrufen, ohne dass eine Anmeldung geprüft wird (**Authentication Bypass by Spoofing, CWE-290**). Laut Volexity führt das über eine Upload-Funktion bis zur **Befehlsausführung ohne Zugangsdaten**. In der beobachteten Kette kombinierten die Angreifer das mit einer weiteren Lücke, die Root-Rechte verschafft – für sie gibt es noch keinen Fix.

ANGRIFFSKETTE

01 Gateway erreichbar – ICS-Anmeldeseite aus dem Internet zugänglich	02 Anmeldung umgangen – gefälschter Header leitet auf geschützte Programme um	03 Code ausgeführt – hochgeladene Datei wird ohne Login ausgeführt	04 Root & Ausbreitung – Rechteausweitung, Mitschnitt, Zugangsdaten, Pivot
--	---	--	---

Betroffenheit & Fixversionen

Produkt / Zweig	Verwundbar bis	Fixversion (Ziel)
ICS 25.1.2.x	≤ 25.1.2.2	25.1.3.0 / 25.1.3.1
ICS 25.1.1.x	≤ 25.1.1.1	25.1.1.2 bzw. 25.1.3.x
ICS 22.8R2	22.8R2 – 22.8R2.4	22.8R2.5
ICS 22.7R2	nicht betroffen	≤ 22.7R2.14 unkritisch

Fixstände laut CVE-Record von Ivanti als CNA (**25.1.3.0 · 25.1.3.1 · 22.8R2.5** nicht betroffen); 25.1.2 als Fix für den 25.1.1-Zweig laut NVD-Auswertung. Die in der Angriffskette zusätzlich genutzte Root-Rechteausweitung behebt Ivanti erst in einem späteren Release – Stand bitte im Hersteller-Advisory prüfen.



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 (UTA0576)

05.10.2026

Volexity untersucht Vorfall

13.10.2026

Advisory mit Fix · CISA-KEV

16.10.2026

CISA-Frist abgelaufen

Ihr Maßnahmenplan.

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

SOFORT

Auf den Fixstand des eigenen Zweigs

KURZFRISTIG

Logs auf Header-Missbrauch prüfen

PARALLEL

Kompromittierung ausschließen

01**Betroffenheit feststellen**

ICS-Version aller Gateways erheben (Admin-Oberfläche → Maintenance → System) und mit der Fixtabelle abgleichen. Internet-erreichbare Gateways haben höchste Priorität.

02**Patchen**

Auf 25.1.3.0 / 25.1.3.1 bzw. 22.8R2.5 aktualisieren. Einen Workaround nennt der Hersteller nicht. Vorher Konfigurationssicherung ziehen.

03**Logs prüfen**

Gehäufte Anfragen an welcome.cgi mit X-DSCGI-PATH-Header, der nicht zur URL passt, sind ein starkes Signal – idealerweise im Proxy/WAF davor mitschneiden und alarmieren.

04**Kompromittierung ausschließen**

Der Integrity Checker kann diese Angriffe übersehen – die Angreifer arbeiten im Arbeitsspeicher. Bei Verdacht Netzwerk- und Speicherforensik, CISA verlangt eine forensische Triage. Der Patch wirkt niemanden hinaus, der schon drin ist.

05**Zugangsdaten als offengelegt behandeln**

Bei Verdacht: Konten, die auf dem Gateway hinterlegt oder darüber genutzt wurden (LDAP-/AD-Dienstkonten, lokale Admins), erneuern und Querbewegungen vom Gateway ins Netz prüfen.

Kompromittierungs-Indikatoren (IoCs)

ANFRAGE-MUSTER

/dana-
na/auth/url_default/welcome.cgi
mit X-DSCGI-PATH auf
.../dana/fb/smb/wu.cgi oder
/home/runtime/tmp/

DATEI-ARTEFAKTE

/data/.icscap/ (Sniffer dsstatmond)
/tmp/ml.py · /tmp/rq5.py ·
/tmp/sp_run.py
/tmp/spray_hits.json

NETZWERK

108.165.147[.]64
Querbewegungen ausgehend
vom ICS-Gateway

Zur Einordnung: Die Indikatoren stammen aus der Analyse von Volexity (13.10.2026), nicht aus dem Hersteller-Advisory. Die IP-Adresse ist eine flüchtige Momentaufnahme; belastbarer sind Header-Missbrauch im Log und Artefakte im Dateisystem. Das Integrity Checker Tool fand in den untersuchten Fällen nichts.



Wichtig: Der Integrity Checker hat diese Angriffe nicht erkannt – die Angreifer patchen Code im Arbeitsspeicher und stellen Konfigurationen wieder her. Ein grünes Prüfergebnis ist hier keine Entwarnung; und die Root-Rechteausweitung der Kette ist noch offen.

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 sowie ausgehende Verbindungen und Anmeldungen 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, deren Anmeldeseite aus dem Internet erreichbar ist – also praktisch jedes produktive ICS-Gateway 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 den Fixstand bringen und den Abschluss bestätigen lassen.
- › Für Gateways, die vor dem Patch 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-2026-104935 und dem Ivanti-Perimeter.

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



Termin buchen