AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-118527

Vorhersagbare Dateinamen in Ivanti Connect Secure: kleiner Wert, wichtiger Baustein der Zero-Day-Kette.

Weil Ivanti Connect Secure vorhersagbare Dateinamen verwendet, können angemeldete Angreifer Dateien mit eigenem Inhalt an einem bekannten Ort ablegen. Für sich genommen ist das nur ein mittleres Risiko – doch CISA führt die Lücke seit dem 30. Oktober 2026 als aktiv ausgenutzt und als verkettbar mit der Zero-Day-Kette um CVE-2026-104935. Der Fix ist seit dem 29. Oktober verfügbar, die CISA-Frist endet am 13. November.

> **Geschäftsrisiko:** Allein begrenzte Wirkung – in der Kette mit CVE-2026-104935 und CVE-2026-111357 droht jedoch die Übernahme des zentralen Fernzugangs samt Zugangsdaten. Ein kompromittiertes Gateway kann einen meldepflichtigen Vorfall nach NIS-2 / DSGVO auslösen.

4,3 / 10

MITTEL
CVSS 3.1 BASISWERT

Niedrig | **Mittel** | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N` – über das Netz, ohne besonderen Aufwand, mit einfachen Rechten; geringe Wirkung auf die Integrität. Basiswert von Ivanti als CNA, vom NVD geführt. Allein ist die Lücke begrenzt – CISA nennt sie verkettbar mit CVE-2026-104935 und CVE-2026-111357.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Oktober 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.

4,3 · MITTEL
CVSS 3.1 (Ivanti · NVD)

Datei-Upload
bekannter Pfad · CWE-340

Aktiv
ausgenutzt · CISA KEV · Frist 13.11.2026

Patch da
seit 29.10.2026

Die Ursache: Ivanti Connect Secure verwendet beim Hochladen **vorhersagbare Dateinamen** (**CWE-340**). Ein angemeldeter Angreifer kann so Dateien mit eigenem Inhalt an einem **bekannten Ort auf dem Datenträger** ablegen. Das passt zu dem von Volexity beschriebenen Muster: Der Upload-Handler **wu.cgi** speichert unter dem MD5-Hash des Dateinamens. Volexity nennt diese CVE-Nummer jedoch nicht – die Zuordnung ist unsere Einordnung.

ANGRIFFSKETTE

01	02	03	04
Anmeldung umgangen – CVE-2026-104935, die Voraussetzung entfällt	**Datei abgelegt** – eigener Inhalt am vorhersagbaren Pfad	**Code ausgeführt** – Aufruf der Datei über den bekannten Pfad	**Root erlangt** – Rechteausweitung über CVE-2026-111357

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	im Record nicht einzeln genannt	s. Hersteller-Advisory

Fixstände **25.1.1.3 · 22.8R2.6** laut CVE-Record von Ivanti als CNA (03.11.2026); die NVD-Auswertung deckt sich damit. Den Zweig 25.1.2 nennt der Record nicht, Volexity führt ihn für die Kette als betroffen – Stand bitte direkt 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 der Kette

29.10.2026
Ivanti-Fix 25.1.1.3 · 22.8R2.6

30.10.2026
CISA-KEV · Frist 13.11.2026

03.11.2026
CVE-Record · CVSS 4,3

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

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

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

01 Betroffenheit feststellen

ICS-Version aller Gateways erheben und mit der Fixtabelle abgleichen. Der Oktober-Patch für CVE-2026-104935 allein reicht nicht.

02 Patchen

Auf `25.1.1.3` bzw. `22.8R2.6` aktualisieren, vorher Konfiguration sichern. Den Wert 4,3 nicht als Grund zum Aufschub nehmen.

03 Spuren suchen

Webserver-Logs auf `X-DSCGI-PATH`-Header prüfen, die auf `/home/runtime/tmp/` zeigen. Lücken in den Logs werten wie ein Treffer.

04 Kompromittierung ausschließen

Das Prüfwerkzeug des Herstellers erkannte die Kette in den untersuchten Fällen nicht. Bei Verdacht Speicher- und Netzwerkforensik.

Kompromittierungs-Indikatoren (IoCs)

ANFRAGE-MUSTER

`…/url_default/welcome.cgi`
mit `X-DSCGI-PATH` auf
`…/dana/fb/smb/wu.cgi`

UPLOAD-PFAD

`/home/runtime/tmp/`
`<MD5(filename)>`
viele parallele Aufrufe

FOLGEARTEFAKTE

`/data/.icscap/dsstatmond`
`/tmp/spray_hits.json`
`108.165.147[.]64`

Zur Einordnung: Die Indikatoren stammen aus der Volexity-Analyse der Gesamtkette (13.10.2026), nicht aus dem Hersteller-Advisory, und sind dieser CVE nicht ausdrücklich zugeordnet. Die IP-Adresse ist eine flüchtige Momentaufnahme; belastbarer sind Header-Missbrauch im Log und Artefakte im Dateisystem.

Wichtig: Der niedrige CVSS-Wert beschreibt die Lücke isoliert, nicht das Risiko der Kette. Und ein grünes Ergebnis des Integrity Checkers ist hier keine Entwarnung – laut Volexity erkennt er diese Kompromittierung nicht.

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 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 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.
- Die Priorität nicht am CVSS-Wert 4,3 festmachen – entscheidend sind die aktive Ausnutzung und die Verkettung mit CVE-2026-104935 und CVE-2026-111357.
- Für Gateways, die im Oktober erreichbar waren, eine forensische Prüfung beauftragen und das Ergebnis für eine etwaige Meldung 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-2026-118527 und dem Ivanti-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: CVE-Record CVE-2026-118527 (Ivanti als CNA) · NVD · CISA KEV (aufgenommen 30.10.2026, Frist 13.11.2026) · Ivanti Security Advisory CVE-2026-104935 · Volexity (13.10.2026, Update 29.10.2026). Stand 05.11.2026 – gegen das Hersteller-Advisory abgleichen.