AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-21887

Command Injection in Ivanti Connect Secure.

In den Web-Komponenten von Ivanti Connect Secure und Policy Secure kann ein Angreifer über präparierte Anfragen beliebige Betriebssystem-Befehle auf dem Gateway ausführen. Verkettet mit dem Authentifizierungs-Bypass CVE-2023-46805 wird daraus eine unauthentifizierte Remote-Code-Ausführung – ohne Zugangsdaten, direkt aus dem Internet. Die Lücke wird seit Ende 2023 aktiv und massenhaft ausgenutzt.

Geschäftsrisiko: vollständige Übernahme des VPN-Gateways am Perimeter – mit Diebstahl von Zugangsdaten und Sitzungen, dauerhaften Webshells, Zugriff auf das interne Netz und einem meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

9,1 / 10

KRITISCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H` – aus dem Netz, ohne Nutzer-Zutun, mit voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit über die Systemgrenze hinaus. Formal ist ein authentifizierter Admin nötig (PR:H) – in Verkettung mit dem Authentifizierungs-Bypass CVE-2023-46805 entfällt diese Hürde und die Lücke wird unauthentifiziert ausnutzbar.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Dezember 2023	Connect Secure 9.x & 22.x Policy Secure 9.x & 22.x	Sofort

Das Wichtigste in 60 Sekunden.

9,1 · KRITISCH
CVSS-Schweregrad

Unauth. RCE
verkettet mit CVE-2023-46805

Aktiv
massenhaft ausgenutzt · CISA KEV · PoC öffentlich

Perimeter
VPN-Gateway aus dem Internet erreichbar

Die Ursache: Die Web-Komponenten der Gateways übergeben Teile eingehender Anfragen ungeprüft an OS-Befehle (CWE-77, Command Injection). Ein authentifizierter Administrator kann so beliebige Kommandos auf der Appliance ausführen. Der zweite Baustein – der Authentifizierungs-Bypass CVE-2023-46805 per Directory-Traversal – hebelt die Anmeldepflicht aus. In Kombination ruft ein völlig unauthentifizierter Angreifer die verwundbare API direkt auf und erreicht Code-Ausführung mit den Rechten des Gateways.

ANGRIFFSKETTE

01	02	03	04
Gateway exponiert – Connect/Policy Secure ist aus dem Internet erreichbar	**Auth-Bypass** – per Traversal (CVE-2023-46805) wird die Anmeldung umgangen	**Command Injection** – präparierte Anfrage schleust OS-Befehle ein (CVE-2024-21887)	**Übernahme** – Webshell, Credential-Diebstahl und Zugriff ins interne Netz

Betroffenheit & Fixversionen

Produkt / Zweig	Verwundbar bis	Fixversion (Ziel)
Connect Secure 9.1	alle 9.x vor Fix	`9.1R14.4 / 9.1R17.2 / 9.1R18.3`
Connect Secure 22.x	22.1–22.6 vor Fix	`22.4R2.2 / 22.5R1.1 / 22.5R2.2`
Policy Secure 9.x / 22.x	alle unterstützten Versionen	Patch je Zweig (ab 31.01.2024)
Interim (vor Patch)	alle Versionen	`mitigation.release.20240107.1.xml`

Betroffen sind laut Hersteller **alle** unterstützten Versionen (9.x und 22.x) beider Produkte. Ivanti gab die Fixes gestaffelt ab dem 31.01.2024 frei; nicht jeder Zweig erhielt sein Patch gleichzeitig. Exakten Fix-Build gegen das Hersteller-Advisory des eigenen Zweigs abgleichen. Wichtig: Der spätere Patch behebt die Lücke, entfernt aber keine bereits platzierten Webshells – vor der Wiederinbetriebnahme Werksreset und Integrity Checker Tool (ICT) einsetzen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff über das Gateway ist regelmäßig ein meldepflichtiger Vorfall – 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

Dez 2023
Gezielte Zero-Day-Angriffe (UTA0178 / Volexity) beobachtet

10.01.2024
Ivanti-Advisory + Interim-Mitigation; Aufnahme in CISA KEV

13.01.2024
Massenhafte Scans und breite Ausnutzung nach Offenlegung

16.01.2024
Öffentlicher Proof-of-Concept verfügbar

31.01.2024
Erste offizielle Patches (u. a. 9.1R14.4, 22.5R1.1)

Ihr Maßnahmenplan.

In dieser Reihenfolge – Mitigation vor Patch, Kompromittierungs-Prüfung vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Mitigation aktivieren / Gerät isolieren	Werksreset + Patch einspielen	Threat Hunting / IoC- & ICT-Abgleich

01 Betroffenheit feststellen

Prüfen, ob Connect Secure oder Policy Secure (9.x oder 22.x) betrieben und aus dem Internet erreichbar ist. Alle unterstützten Versionen gelten als verwundbar – auch wenn kein direkter Angriff sichtbar ist.

02 Sofort mitigieren (vor dem Patch)

Die von Ivanti bereitgestellte Interim-Mitigation über das Portal einspielen:

```
import mitigation.release.20240107.1.xml
```

03 Kompromittierung prüfen

Das Ivanti Integrity Checker Tool (ICT) ausführen und Auth-/Web-Logs auf die IoCs unten abgleichen. Achtung: Angreifer haben die Mitigation umgangen und das ICT teils getäuscht – ein sauberes ICT-Ergebnis ist kein Freibrief.

04 Werksreset + Patchen

Vor dem Patch einen Werksreset durchführen, um eventuell platzierte Webshells zu entfernen, dann auf die Fixversion des eigenen Zweigs aktualisieren (`9.1R14.4` · `9.1R17.2` · `9.1R18.3` · `22.4R2.2` · `22.5R1.1` · `22.5R2.2`).

05 Zugangsdaten rotieren

Nach bestätigter oder vermuteter Kompromittierung alle auf dem Gateway gespeicherten und darüber genutzten Geheimnisse zurücksetzen: lokale Konten, Service-Accounts, API-Schlüssel und Zertifikate. Der Credential-Harvester WARPWIRE greift Klartext-Anmeldungen ab.

Kompromittierungs-Indikatoren (IoCs)

EXPLOIT-PFAD (TRAVERSAL → API)

`/api/v1/totp/user-backup-code/../../license/keys-status/<cmd>`

BEOBACHTETE MALWARE-FAMILIEN

Webshells `WIREFIRE`, `GIFTEDVISITOR`, `LIGHTWIRE`

Credential-Harvester `WARPWIRE`

PRÜF-SIGNALE

ICT-Abweichungen / neue Dateien in `/home/webserver/htdocs`

manipulierte `compcheck.cgi` / `visits.py`

Zur Einordnung: Die Angreifer haben die Interim-Mitigation umgangen und das Integrity Checker Tool teils getäuscht; Malware-Namen und Pfade sind eine Momentaufnahme der beobachteten Kampagnen und flüchtig. Ein sauberes ICT-Ergebnis ersetzt keine gründliche forensische Analyse – im Zweifel Werksreset vor Wiederinbetriebnahme.

Wichtig: Ein reiner Patch genügt nicht: Wer vor dem Update kompromittiert wurde, behält die Webshells auch nach dem Einspielen. Ivanti und CISA empfehlen ausdrücklich Werksreset und Credential-Rotation vor der Wiederinbetriebnahme.

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: Traversal-Anfragen an die Lizenz-/TOTP-API und neue Dateien in den Web-Verzeichnissen des Gateways 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 Ivanti-Gateways 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 Connect Secure-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

- Mitigation heute anordnen, betroffene Gateways als kompromittiert behandeln bis zum Gegenbeweis.
- Werksreset, Patch und Credential-Rotation als ein Vorgang einplanen – nicht nur patchen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung nach NIS-2 / DSGVO.

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-2024-21887 und dem Connect Secure-Perimeter.

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

Termin buchen

Quellen: Ivanti Security Advisory (Forums-KB CVE-2023-46805 / CVE-2024-21887) · NVD (CVE-2024-21887, CVSS 3.1 9,1) · CISA KEV (hinzugefügt 10.01.2024, Frist 22.01.2024) · CISA Alert & Emergency Directive ED 24-01 · Volexity- und Mandiant-Analysen · Unit 42 Threat Brief · Tenable / Rapid7 Berichte. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.