AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-21893

Unauthentifizierte SSRF im SAML-Modul von Ivanti Connect Secure.

Ein nicht authentifizierter Angreifer aus dem Internet kann über die SAML-Komponente serverseitige Anfragen erzwingen (SSRF) und so auf abgeschottete interne Dienste zugreifen. In der Praxis wird die Lücke mit der Command-Injection CVE-2024-21887 verkettet – das Ergebnis ist unauthentifizierte Codeausführung auf der Appliance. Die Ausnutzung läuft seit Ende Januar 2024.

> **Geschäftsrisiko:** vollständige Übernahme des VPN-Gateways und damit unbefugter Zugang zum internen Netz – mit Potenzial für Datenabfluss, Persistenz, Betriebsunterbrechung und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

8,2 / 10

HOCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | **Hoch** | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N` – aus dem Netz, ohne Rechte, ohne Zutun – mit hohem Verlust der Vertraulichkeit. Ein CVSS-4.0-Wert liegt für diese Schwachstelle nicht vor; Basis ist der offizielle CVSS-3.1-Wert des NVD.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Ende Januar 2024	Connect Secure & Policy Secure 9.x / 22.x + Neurons for ZTA	Sofort

Das Wichtigste in 60 Sekunden.

8,2 · HOCH
CVSS 3.1 Basiswert

SSRF
SAML-Komponente · unauthentifiziert

Aktiv
ausgenutzt · CISA KEV · PoC öffentlich

Kettbar
mit CVE-2024-21887 → RCE

Die Ursache: Die SAML-Komponente von Connect Secure, Policy Secure und Neurons for ZTA verarbeitet eingehende SOAP-/XML-Nachrichten mit einer verwundbaren `xmltooling`-Bibliothek. Über präparierte `KeyInfo`-Elemente mit einer `RetrievalMethod`-URI lässt sich der Server dazu bringen, beliebige serverseitige Anfragen auszuführen (Server-Side Request Forgery, CWE-918). Da hierfür keine Authentifizierung nötig ist, erreicht ein Angreifer interne Dienste, die von außen eigentlich nicht erreichbar sind.

ANGRIFFSKETTE

01	02	03	04
Portal exponiert – Connect/Policy Secure ist aus dem Internet erreichbar	**SSRF auslösen** – präparierte SOAP-/SAML-Nachricht an den SAML-Endpunkt senden	**Verketten** – interne API über die SSRF mit CVE-2024-21887 (Command Injection) ansteuern	**RCE** – unauthentifizierte Codeausführung auf der Appliance

Betroffenheit & Fixversionen

Produkt / Zweig	Verwundbar bis	Fixversion (Ziel)
Connect Secure 9.1R	< 9.1R14.4 / 9.1R17.2 / 9.1R18.3	9.1R14.4 · 9.1R17.2 · 9.1R18.3
Connect Secure 22.x	< 22.4R2.2 / 22.5R1.1 / 22.5R2.2	22.4R2.2 · 22.5R1.1 · 22.5R2.2
Policy Secure 22.x	< 22.5R1.1	22.5R1.1
Neurons for ZTA	< 22.6R1.3	22.6R1.3

Betroffen sind alle unterstützten 9.x- und 22.x-Zweige von Connect Secure und Policy Secure sowie Neurons for ZTA. Exakte Build-Ranges gegen das Hersteller-Advisory des eigenen Zweigs abgleichen – Ivanti hat die Fixes gestaffelt über mehrere Release-Züge ausgeliefert.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff oder eine RCE auf dem Gateway kann eine meldepflichtige Verletzung darstellen – 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

31.01.2024
Ivanti veröffentlicht Advisory (CVE-2024-21888 & CVE-2024-21893) + Patches

31.01.2024
CISA nimmt die Lücke in den KEV-Katalog auf (Frist Behörden: 02.02.2024)

Anf. Feb. 2024
Ivanti & Mandiant bestätigen aktive Ausnutzung – SSRF umgeht frühere Mitigation

Seither
Öffentliche PoCs; Verkettung mit CVE-2024-21887 zu unauth. RCE

Ihr Maßnahmenplan.

In dieser Reihenfolge – Mitigation vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Mitigation aktivieren	Patch einspielen	Integritätsprüfung & Threat Hunting

01 Betroffenheit feststellen

Prüfen, welche Ivanti-Appliances (Connect Secure, Policy Secure, Neurons for ZTA) aus dem Internet erreichbar sind und auf welchem Release-Zweig sie laufen. Alle nicht auf einer Fixversion befindlichen Instanzen sind angreifbar.

02 Sofort mitigieren (vor dem Patch)

Sofern noch nicht gepatcht werden kann, die von Ivanti bereitgestellte Mitigation (Import der Hersteller-Mitigation-XML über das Admin-Portal) einspielen. Wird SAML nicht benötigt, die betroffene Komponente entsprechend einschränken. Die Mitigation ist ein Behelf – kein Ersatz für den Patch.

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (`Connect Secure 9.1R14.4 · 9.1R17.2 · 9.1R18.3 · 22.4R2.2 · 22.5R1.1 · 22.5R2.2`; `Policy Secure 22.5R1.1`; `ZTA 22.6R1.3`). Die Fixversion schließt CVE-2024-21893 zusammen mit den weiteren Ivanti-Lücken dieser Welle.

04 Kompromittierung ausschließen

Nach dem Patch einen Factory Reset gemäß Ivanti-Empfehlung erwägen und den Ivanti Integrity Checker Tool (ICT) laufen lassen. Auth- und Web-Logs auf Zugriffe auf die SAML-/interne-API-Endpunkte aus unerwarteten Quellen durchsuchen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Perimeter dauerhaft überwachen

Herstellerseitige IPS-/Threat-Prevention-Signaturen für diese Schwachstelle einspielen, sofern verfügbar. Exponierte VPN-Gateways kontinuierlich auf anomale Zugriffe und Integritätsverletzungen überwachen.

Kompromittierungs-Indikatoren (IoCs)

SSRF-ENDPUNKT (SAML)

`/dana-ws/saml20.ws`

VERKETTETES ZIEL (RCE)

Command-Injection über `CVE-2024-21887`
interne API-Aufrufe wie `/api/v1/license/keys-status`

INTEGRITÄTSPRÜFUNG

Abweichungen im Ivanti `Integrity Checker Tool (ICT)`
unerwartete Ausgänge / neue Dateien auf der Appliance

Zur Einordnung: Die genannten Endpunkte sind reguläre Bestandteile der Appliance – auffällig nur in Verbindung mit unauthentifizierten Zugriffen aus fremden Quellen. Belastbare, veröffentlichte Angreifer-IPs für genau diese Schwachstelle liegen nicht in gesicherter Form vor; maßgeblich sind die Analyse Ihrer eigenen Web-/Auth-Logs und das Ergebnis des Ivanti Integrity Checker Tool.

Wichtig: Die SSRF selbst hinterlässt kaum auffällige Spuren – gefährlich wird sie durch die Verkettung mit CVE-2024-21887 zur RCE. Angreifer haben zudem gezeigt, dass sie frühere Mitigations umgehen konnten; nur der Patch (plus Integritätsprüfung) gibt belastbare Sicherheit.

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: Unauthentifizierte Zugriffe auf die SAML-/interne-API-Endpunkte und ICT-Integritätswarnungen fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, 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 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

- Mitigation heute anordnen, Patch kurzfristig einspielen – exponierte Gateways zuerst.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist (ICT + Log-Analyse), dokumentiert für eine etwaige Meldung.
- Über eine dauerhafte Überwachung des Perimeters entscheiden.

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-2024-21893 und dem Ivanti-Perimeter.

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

Termin buchen

Quellen: NVD (CVE-2024-21893, CVSS 3.1 8,2) · Ivanti Security Advisory / Security Update Blog · Rapid7 Analysis · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 31.01.2024). 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.