AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-0282

Unauthentifizierte Remote-Code-Ausführung in Ivanti Connect Secure.

Ein nicht authentifizierter Angreifer aus dem Internet kann über einen Stack-Pufferüberlauf beliebigen Code auf einer Ivanti-Connect-Secure-Appliance ausführen – ohne Anmeldedaten und ohne Zutun eines Nutzers. Die Lücke wurde bereits vor der Veröffentlichung als Zero-Day gegen internetseitige VPN-Gateways ausgenutzt.

> **Geschäftsrisiko:** vollständige Übernahme des VPN-Gateways am Perimeter – mit Potenzial für Ausbreitung ins interne Netz, Diebstahl von Zugangsdaten, Ransomware und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

9,0 / 10

KRITISCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H` – aus dem Netz, ohne Anmeldung, ohne Zutun des Nutzers – mit vollständiger Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit und Ausbruch aus dem betroffenen Systemkontext. Übereinstimmend von NVD und Ivanti bewertet.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Mitte Dezember 2024	Connect Secure 22.7R2 – 22.7R2.4 + Policy Secure & ZTA Gateways	Sofort

Das Wichtigste in 60 Sekunden.

9,0 · KRITISCH
CVSS-Schweregrad

Unauth RCE
Stack-Pufferüberlauf, ohne Anmeldung

Zero-Day
aktiv ausgenutzt · CISA KEV · Ransomware

Perimeter
internetseitiges VPN-Gateway

Die Ursache: In den betroffenen Versionen prüft der VPN-Dienst die Länge einer bestimmten, ohne Anmeldung erreichbaren Eingabe nicht ausreichend. Eine überlange Anfrage überschreibt den Stack-Speicher (`CWE-121` / `CWE-787`) und lenkt den Programmablauf um. So kann ein Angreifer aus dem Internet eigenen Code ausführen – ohne gültiges Konto und ohne dass ein Nutzer aktiv werden muss.

ANGRIFFSKETTE

01
Gateway exponiert – Connect Secure ist aus dem Internet erreichbar

02
Überlange Anfrage – präparierter Request überläuft den Stack-Puffer

03
Code-Ausführung – eigener Code läuft ohne Anmeldung auf der Appliance

04
Festsetzen – Malware (SPAWN-Familie), Web-Shells, Diebstahl von Zugangsdaten

Betroffenheit & Fixversionen

Produkt / Zweig	Verwundbar bis	Fixversion (Ziel)
Connect Secure	`22.7R2 – 22.7R2.4`	`22.7R2.5`
Policy Secure	`22.7R1 – 22.7R1.2`	`22.7R1.2 (ab 21.01.2025)`
Neurons for ZTA Gateways	`22.7R2 – 22.7R2.3`	`22.7R2.5 (ab 21.01.2025)`
Ausnutzung beobachtet	nur Connect Secure	—

Aktiv ausgenutzt wurde bislang ausschließlich **Connect Secure**. Der Patch für Connect Secure (`22.7R2.5`) stand zur Veröffentlichung bereit; die Fixes für Policy Secure und ZTA Gateways folgten zum 21.01.2025. Version 22.2 und ältere Zweige sind nicht mehr im Support – Migration prüfen. Exakte Build-Ranges und Fixstände gegen das Hersteller-Advisory abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff über das VPN-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

Dez. 2024
Erste Ausnutzung als Zero-Day gegen Connect Secure (Mandiant)

08.01.2025
Ivanti veröffentlicht Advisory · Connect-Secure-Patch verfügbar

08.01.2025
CISA nimmt CVE in den KEV-Katalog auf (Frist 15.01.2025)

21.01.2025
Fixes für Policy Secure und ZTA Gateways verfügbar

Ihr Maßnahmenplan.

In dieser Reihenfolge – Integrität prüfen, patchen, erst dann Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
ICT-Scan + Betroffenheit	Patch einspielen (Factory Reset)	Threat Hunting / Kompromittierung ausschließen

01 Betroffenheit feststellen

Prüfen, ob Connect Secure, Policy Secure oder ein Neurons-for-ZTA-Gateway in einer betroffenen 22.7-Version im Einsatz ist und ob es aus dem Internet erreichbar ist. Priorität hat jede internetseitig exponierte Connect-Secure-Appliance – nur dort wurde bislang aktive Ausnutzung beobachtet.

02 Integrität prüfen (vor allem anderen)

Den Ivanti Integrity Checker Tool (ICT) ausführen – bevorzugt den externen Scan. Ein auffälliges ICT-Ergebnis deutet auf eine Kompromittierung hin und ändert das weitere Vorgehen: Dann ist ein Vorfall zu behandeln, nicht nur zu patchen.

03 Patchen

Connect Secure auf `22.7R2.5` aktualisieren. Policy Secure (`22.7R1.2`) und ZTA Gateways (`22.7R2.5`) auf die ab 21.01.2025 bereitgestellten Fixstände heben. Ivanti empfiehlt bei sauberem ICT ein Werks-Reset (Factory Reset) vor der Wiederinbetriebnahme, um Persistenz auszuschließen.

04 Kompromittierung ausschließen

Bei auffälligem ICT-Ergebnis oder Anzeichen einer Ausnutzung: Appliance vom Netz nehmen, forensisch sichern, betroffene und über das VPN erreichbare Systeme untersuchen und alle über das Gateway nutzbaren Zugangsdaten und Zertifikate/Secrets rotieren. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Perimeter härten

Zugriff auf das Management-Interface einschränken, Exposition des Portals minimieren und die Auswertung von Appliance- und VPN-Logs dauerhaft aufsetzen. Nicht mehr unterstützte Ivanti-Versionen (22.2 und älter) mit Migrationsplan ablösen.

Kompromittierungs-Indikatoren (IoCs)

PRIMÄRES PRÜFMITTEL

Ivanti `Integrity Checker Tool (ICT)`
externer Scan bevorzugt

MALWARE (MANDIANT)

SPAWN-Ökosystem: `SPAWNANT` · `SPAWNMOLE` · `SPAWNSNAIL`
zusätzlich `PHASEJAM`, `DRYHOOK`

VERHALTENS-MARKER

fehlgeschlagene/auffällige ICT-Läufe
unerwartete Neustarts, Web-Shells, Log-Manipulation

Zur Einordnung: Ein sauberes ICT-Ergebnis ist kein vollständiger Freibrief – der Scan erfasst eine Momentaufnahme und kann von einem versierten Angreifer umgangen werden. Die genannten Malware-Familien stammen aus der Analyse von Mandiant (Google Threat Intelligence) und sind eine Momentaufnahme der beobachteten Kampagne. Maßgeblich bleibt die Analyse Ihrer eigenen Appliance- und Netzwerk-Logs.

Wichtig: Aktiv ausgenutzt wurde die Lücke bereits vor Veröffentlichung des Patches (Zero-Day). Ein alleiniges Einspielen des Updates entfernt eine bereits eingerichtete Persistenz nicht – ohne Integritätsprüfung und ggf. Werks-Reset bleibt ein erfolgter Zugriff unsichtbar.

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: Auffällige ICT-Ergebnisse, anomale VPN-Sessions und ungewöhnliche Prozesse auf der Appliance fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden internetseitige, ungepatchte Ivanti-Connect-Secure-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

- Sofort ICT-Scan aller exponierten Ivanti-Gateways anordnen und internetseitige Connect-Secure-Appliances priorisiert patchen.
- Bei Auffälligkeiten Kompromittierung untersuchen lassen – dokumentiert für eine etwaige Meldung nach DSGVO / NIS-2.
- Über eine dauerhafte Überwachung des Perimeters und die Ablösung nicht mehr unterstützter Versionen 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-2025-0282 und dem Ivanti-Perimeter.

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

Termin buchen

Quellen: NVD (nvd.nist.gov/vuln/detail/CVE-2025-0282) · Ivanti Security Advisory (Connect Secure / Policy Secure / ZTA Gateways, CVE-2025-0282 / CVE-2025-0283) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 08.01.2025, Ransomware-Nutzung „bekannt") · Mandiant / Google Threat Intelligence (Zero-Day-Ausnutzung ab Dez. 2024, SPAWN-Malware). Angaben nach bestem Wissen zum Stand 14.07.2026; das Hersteller-Advisory war zum Redaktionszeitpunkt nicht direkt abrufbar – Fixversionen, Build-Ranges und Verfügbarkeitstermine vor dem Patchen gegen das Ivanti-Advisory des jeweiligen Produkts verifizieren. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.