AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-22457

Unauthentifizierte Remote-Code-Ausführung in Ivanti Connect Secure.

Ein nicht authentifizierter Angreifer aus dem Internet kann über einen Stack-Buffer-Overflow eigenen Code auf dem Gerät ausführen – ohne Zugangsdaten, ohne Nutzerinteraktion. Die China-nahe Gruppe UNC5221 hat den ursprünglich als harmlos eingestuften Fehler durch Reverse-Engineering des Patches waffenfähig gemacht und nutzt ihn seit Mitte März 2025 aktiv aus.

> **Geschäftsrisiko:** vollständige Übernahme des VPN-Gateways am Perimeter – mit Potenzial für Netzwerk-Einbruch, Datenabfluss, Persistenz durch Malware und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

9,8 / 10

KRITISCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` – aus dem Netz, ohne Rechte, ohne Zutun, mit vollständiger Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. NVD bewertet mit 9,8 (kritisch); Ivanti selbst mit 9,0.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Mitte März 2025	Connect Secure ≤ 22.7R2.5 Policy Secure, ZTA Gateways + EOL 9.x	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (NVD)

Unauth RCE
Stack-Buffer-Overflow, Perimeter

Aktiv
ausgenutzt · CISA KEV · Ransomware bekannt

UNC5221
China-nahe Spionagegruppe

Die Ursache: Ein Handler in Connect Secure prüft die Länge einer eingehenden Eingabe nicht ausreichend und schreibt über die Grenzen eines Stack-Puffers hinaus (**Stack-Based Buffer Overflow**, CWE-121 / CWE-787). Ivanti hielt den Fehler zunächst für einen nicht ausnutzbaren Denial-of-Service und schloss ihn still in 22.7R2.6. UNC5221 verglich den Patch mit der Vorversion, rekonstruierte die Schwachstelle und entwickelte einen zuverlässigen Weg zur Code-Ausführung – gegen ungepatchte Systeme.

ANGRIFFSKETTE

01
Gateway exponiert – Connect Secure ist aus dem Internet erreichbar

02
Overflow auslösen – überlange Eingabe sprengt den Stack-Puffer

03
Code ausführen – In-Memory-Dropper TRAILBLAZE injiziert die Backdoor BRUSHFIRE

04
Persistenz & Tarnung – SPAWN-Malware klinkt sich ein, Logs werden manipuliert

Betroffenheit & Fixversionen

Produkt / Zweig	Verwundbar bis	Fixversion (Ziel)
Connect Secure	≤ 22.7R2.5 (inkl. EOL 9.x)	22.7R2.6
Policy Secure	< 22.7R1.4	22.7R1.4
ZTA Gateways	< 22.8R2.2	22.8R2.2
Neurons for Secure Access	betroffen – Rollout über Ivanti	Patch-Status mit Ivanti abstimmen

Der Patch für Connect Secure (22.7R2.6) wurde bereits am 11.02.2025 veröffentlicht; die Fixes für Policy Secure und ZTA Gateways folgten Mitte/Ende April 2025. End-of-Life-Versionen der Zscaler-9.x-Reihe erhalten keine Fixes und müssen migriert werden. Exakte Build-Ranges gegen das Hersteller-Advisory abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf ein Perimeter-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

11.02.2025
Ivanti veröffentlicht 22.7R2.6 – Fehler als DoS eingestuft, still gepatcht

Mitte März 2025
UNC5221 beginnt aktive Ausnutzung ungepatchter Systeme

03.04.2025
Ivanti-Advisory & Mandiant-Analyse zur RCE-Ausnutzung

04.04.2025
Aufnahme in CISA KEV · Ransomware-Bezug bekannt

April 2025
Fixes für Policy Secure (22.7R1.4) und ZTA Gateways (22.8R2.2)

Ihr Maßnahmenplan.

In dieser Reihenfolge – Patch vor Entwarnung, Kompromittierung immer ausschließen.

SOFORT	SOFORT	PARALLEL
Fixversion einspielen	Integrity Checker Tool (ICT) laufen lassen	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

Version und Produkt aller Ivanti-Gateways erfassen: Connect Secure ≤ 22.7R2.5, Policy Secure < 22.7R1.4, ZTA Gateways < 22.8R2.2 sowie sämtliche EOL-9.x-Systeme sind angreifbar. Aus dem Internet erreichbare Instanzen zuerst behandeln.

02 Patchen

Auf die Fixversion des jeweiligen Produkts aktualisieren (`Connect Secure 22.7R2.6` · `Policy Secure 22.7R1.4` · `ZTA 22.8R2.2`). EOL-9.x-Systeme erhalten keinen Fix und müssen auf eine unterstützte Linie migriert werden.

03 Kompromittierung ausschließen

Das Ivanti Integrity Checker Tool (ICT) ausführen und auf Statedump-Dateien sowie Core-Dumps des `web`-Prozesses prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Einbruch. Bei Verdacht Factory-Reset auf sauberer Firmware, nicht nur Upgrade.

04 IoCs & Malware abgleichen

Auf die Post-Exploitation-Familien TRAILBLAZE (In-Memory-Dropper), BRUSHFIRE (Backdoor) und das SPAWN-Ökosystem (SPAWNSLOTH/SPAWNSNARE/SPAWNWAVE) prüfen. Die IoCs unten und die Hashes aus dem Mandiant-Bericht heranziehen.

05 Perimeter dauerhaft überwachen

UNC5221 zielt gezielt auf Edge-Geräte. Kontinuierliche Auswertung der Gateway-Logs, Anomalie-Erkennung auf ungewöhnliche TLS-Client-Zertifikate und Alarmierung bei Integritätsabweichungen etablieren.

Kompromittierungs-Indikatoren (IoCs)

TRAILBLAZE (DROPPER)	BRUSHFIRE (BACKDOOR)	SPAWN-FAMILIE
`/tmp/.i`	`/tmp/.r`	`/bin/dsmain` ·
MD5	MD5	`/lib/libdsupgrade.so`
`4628a501088c31f53b5c9ddf6788e835`	`e5192258c27e712c7acf80303e68980b`	`/tmp/.liblogblock.so`

Zur Einordnung: Die Hashes und Dateipfade stammen aus der von Mandiant analysierten Kampagne und sind flüchtig – kein Ersatz für den Lauf des Integrity Checker Tools und die Analyse Ihrer Gateway-Logs. SPAWNSLOTH manipuliert lokales Logging und Syslog-Weiterleitung; fehlende Logs sind selbst ein Warnzeichen.

Wichtig: Der Fehler wurde als DoS unterschätzt und still gepatcht – Angreifer haben genau diesen Patch analysiert, um die RCE zu entwickeln. Wer 22.7R2.6 nicht eingespielt hat, ist gegen eine bereits waffenfähige, aktiv genutzte Schwachstelle exponiert. Die eingesetzte Malware deaktiviert zudem Logs; ein Einbruch bleibt ohne Integritätsprüfung 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: Integritätsabweichungen am Gateway, Core-Dumps des web-Prozesses und anomale TLS-Client-Zertifikate 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-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

- Patch der Perimeter-Gateways sofort anordnen, EOL-9.x-Systeme umgehend migrieren.
- Kompromittierung per Integrity Checker Tool ausschließen lassen – dokumentiert für eine etwaige Meldung.
- Über eine dauerhafte Überwachung der Edge-Geräte entscheiden – UNC5221 zielt wiederholt darauf.

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-2025-22457 und dem Ivanti-Perimeter.

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

Termin buchen

Quellen: Ivanti April Security Advisory CVE-2025-22457 · NVD (CVSS 3.1 9,8) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 04.04.2025, Ransomware-Bezug bekannt) · Google/Mandiant Threat Intelligence (UNC5221, TRAILBLAZE/BRUSHFIRE/SPAWN). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory des jeweiligen Produkts abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.