AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-8190

OS-Command-Injection in Ivanti Cloud Services Appliance.

Ein Angreifer mit Admin-Rechten der CSA-Verwaltungskonsole kann über eine OS-Command-Injection beliebige Betriebssystem-Befehle auf der Appliance ausführen. In der beobachteten Angriffswelle wurde die Lücke mit der Auth-Bypass-Schwachstelle CVE-2024-8963 verkettet – so wird aus der Admin-Voraussetzung ein nicht authentifizierter Fernzugriff bis zur Codeausführung. CSA 4.6.x ist End-of-Life.

> **Geschäftsrisiko:** vollständige Übernahme der Appliance mit Webshell-Persistenz, Zugriff auf verwaltete Endpunkte und Zugangsdaten – mit Potenzial für Datenabfluss, Lateral Movement und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

7,2 / 10

HOCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | **Hoch** | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H` – aus dem Netz, mit Admin-Rechten der Appliance, ohne Zutun des Opfers, mit voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Kein CVSS-4.0-Wert von NVD/Ivanti veröffentlicht.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
September 2024 (Zero-Day)	CSA 4.6 (Patch 518 & älter) Fix: 4.6 Patch 519 · 5.0.x nicht betroffen	Sofort

Das Wichtigste in 60 Sekunden.

7,2 · HOCH
CVSS 3.1 Basiswert

OS-Command-Injection
Admin-Konsole der CSA

Aktiv
ausgenutzt · CISA KEV · PoC öffentlich

EOL
CSA 4.6.x – nur noch 5.0.x supportet

Die Ursache: Die Verwaltungskonsole der CSA übergibt Eingabewerte ungeprüft an einen Betriebssystem-Aufruf (CWE-78). Ein an der Appliance angemeldeter Administrator kann so eigene Befehle einschleusen und mit den Rechten des Web-Dienstes ausführen. Für sich genommen verlangt die Lücke Admin-Rechte (`PR:H`) – in der realen Ausnutzung wird sie jedoch mit dem Path-Traversal- bzw. Auth-Bypass `CVE-2024-8963` verkettet, der diese Hürde entfernt.

ANGRIFFSKETTE

01	02	03	04
Konsole erreichbar – CSA-Verwaltungsoberfläche aus dem Netz exponiert	**Auth umgehen** – Path Traversal `CVE-2024-8963` verschafft Zugang zu Admin-Funktionen	**Befehl einschleusen** – OS-Command-Injection `CVE-2024-8190` führt Code auf der Appliance aus	**Persistenz** – Webshell abgelegt, Zugangsdaten abgegriffen, Konten manipuliert

Betroffenheit & Fixversionen

CSA-Version	Verwundbar bis	Fixversion (Ziel)
CSA 4.6	≤ 4.6 Patch 518	4.6 Patch 519
CSA 5.0.x	nicht betroffen	—

CSA 4.6.x hat den **End-of-Life**-Status erreicht: Patch 519 ist der letzte Fix für diesen Zweig, künftige Lücken erhalten voraussichtlich keine Updates mehr. Ivanti und CISA empfehlen, 4.6.x außer Betrieb zu nehmen oder auf die supportete 5.0.x-Linie zu migrieren. Exakte Build-Angaben gegen das Hersteller-Advisory abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff oder eine Webshell auf der Appliance 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

10.09.2024
Ivanti veröffentlicht Advisory + Patch 519

13.09.2024
CISA KEV · Ivanti bestätigt begrenzte Ausnutzung

16.09.2024
Öffentliches Exploit-Skript / PoC verfügbar

19.09.2024
CVE-2024-8963 (Auth-Bypass) gemeldet – Kette für unauth. RCE

22.01.2025
CISA/FBI Joint Advisory AA25-022A zu Exploit-Ketten

Ihr Maßnahmenplan.

In dieser Reihenfolge – Exposition zuerst schließen, dann patchen oder migrieren.

SOFORT	KURZFRISTIG	PARALLEL
Konsole vom Internet trennen	Patch 519 bzw. Migration 5.0.x	Threat Hunting / Kompromittierung prüfen

01 Betroffenheit feststellen

Prüfen, ob eine Ivanti CSA 4.6.x im Einsatz ist und ob die Verwaltungskonsole aus dem Internet erreichbar ist. Version und Patch-Stand ermitteln – angreifbar sind alle Builds bis einschließlich `4.6 Patch 518`.

02 Exposition sofort reduzieren

Den Zugriff auf die Verwaltungskonsole vom Internet abtrennen bzw. auf vertrauenswürdige Management-Netze einschränken. Da die Lücke mit `CVE-2024-8963` zum unauthentifizierten Zugriff verkettet wird, ist die Reduktion der Erreichbarkeit die wirksamste Sofortmaßnahme.

03 Patchen oder migrieren

Auf `4.6 Patch 519` aktualisieren. Da CSA 4.6.x End-of-Life ist, sollte parallel die Migration auf die supportete `5.0.x`-Linie geplant werden – 5.0.x ist von dieser Schwachstelle nicht betroffen.

04 Kompromittierung ausschließen

Nach dem Patch verbleibt das Risiko eines bereits erfolgten Zugriffs. Appliance auf Webshells, unbekannte Admin-Konten und anomale Befehlsausführung untersuchen; Logs der Konsole und der unten genannten Endpunkte prüfen. Bei Verdacht: Appliance als kompromittiert behandeln, neu aufsetzen und Zugangsdaten rotieren.

05 Verkettete Lücken mitbehandeln

Im selben Wartungsfenster auch `CVE-2024-8963` (Auth-Bypass) sowie die zeitgleich gemeldeten `CVE-2024-9379` / `CVE-2024-9380` berücksichtigen – Patch 519 adressiert die Kernkette. Herstellerangaben zum jeweiligen Zweig maßgeblich.

Kompromittierungs-Indikatoren (IoCs)

EINSCHLEUSUNGS-VEKTOR

OS-Command-Injection über die DateTime-/TIMEZONE-Funktion der Admin-Konsole

VERKETTETE LÜCKE

Path Traversal `CVE-2024-8963` (Auth-Bypass zu Admin-Funktionen)

NACHLAUF-AKTIVITÄT

neu abgelegte Webshells · unbekannte Admin-Konten · anomale Befehlsausführung

Zur Einordnung: Die Angaben beschreiben das Angriffsmuster der beobachteten Kampagne (CISA/FBI AA25-022A) und sind kein Ersatz für die forensische Analyse der Appliance und ihrer Logs. Konkrete Datei-Pfade, Hashes und IPs bitte dem aktuellen CISA-Advisory und Ihren eigenen Protokollen entnehmen.

Wichtig: Für sich genommen setzt die Lücke Admin-Rechte voraus – in der Praxis wurde sie jedoch als Zero-Day mit einem Auth-Bypass verkettet und für unauthentifizierten Fernzugriff genutzt. Ein Patch schließt die Lücke, entfernt aber keine bereits abgelegte Webshell.

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: Anomale Befehlsausführung auf der Appliance und neu angelegte Admin-Konten oder Webshells fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte CSA-4.6.x-Verwaltungskonsolen 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 CSA-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

- Erreichbarkeit der CSA-Konsole heute prüfen und einschränken, Patch 519 kurzfristig einspielen.
- Migration von der End-of-Life-Version 4.6.x auf die supportete 5.0.x-Linie beschließen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.

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-2024-8190 und dem Ivanti CSA-Perimeter.

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

Termin buchen

Quellen: NVD CVE-2024-8190 (CVSS 3.1 7,2, Vektor, betroffene/Fix-Versionen) · Ivanti Security Advisory Cloud Services Appliance (CSA) CVE-2024-8190 · CISA Known Exploited Vulnerabilities Catalog (Aufnahme 13.09.2024, Frist 04.10.2024) · CISA/FBI Joint Cybersecurity Advisory AA25-022A (Exploit-Ketten). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.