AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-9380

OS-Command-Injection in Ivanti Cloud Services Appliance.

Ein authentifizierter Angreifer mit Administrator-Rechten in der Web-Konsole der Ivanti Cloud Services Appliance kann beliebige Betriebssystem-Befehle ausführen und das Gerät vollständig übernehmen. In freier Wildbahn wird die Lücke mit der Auth-Bypass-Schwachstelle CVE-2024-8963 verkettet – der Angreifer verschafft sich die nötigen Admin-Rechte damit selbst und braucht keine gültigen Zugangsdaten.

> **Geschäftsrisiko:** vollständige Übernahme des internetnahen CSA-Gateways mit Webshell-Persistenz, Diebstahl von Administrator-Zugangsdaten und Brückenkopf ins interne Netz – mit Potenzial für Datenabfluss, Betriebsunterbrechung 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 erreichbar, geringe Angriffskomplexität, ohne Nutzerzutun – erfordert für sich genommen Administrator-Rechte (PR:H) und wirkt dann voll auf Vertraulichkeit, Integrität und Verfügbarkeit. In der beobachteten Praxis wird die Rechte-Voraussetzung durch die vorgeschaltete Auth-Bypass-Lücke CVE-2024-8963 umgangen.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Oktober 2024	Ivanti CSA 5.0.1 und älter	Sofort

Das Wichtigste in 60 Sekunden.

7,2 · HOCH
CVSS 3.1 Basiswert

OS Command Injection
Admin-Web-Konsole (authentifiziert)

Aktiv
ausgenutzt · CISA KEV · Exploit-Kette

Fix: 5.0.2
CSA 5.0.1 & älter betroffen

Die Ursache: Die Admin-Web-Konsole der CSA übergibt Nutzereingaben unzureichend gefiltert an einen Betriebssystem-Aufruf (CWE-78). Ein Angreifer mit Zugriff auf die Konsole kann eigene Befehle einschleusen, die das Gerät mit den Rechten des Web-Dienstes ausführt. Die eigentlich nötigen Administrator-Rechte beschafft sich der Angreifer in der beobachteten Kampagne über die vorgeschaltete Authentifizierungs-Umgehung CVE-2024-8963 – die Kette macht aus einer authentifizierten eine faktisch nicht authentifizierte Übernahme.

ANGRIFFSKETTE

01
Auth-Bypass – Zugriff auf die Admin-Konsole ohne gültige Anmeldung über CVE-2024-8963

02
Command Injection – beliebige OS-Befehle über die Konsole (CVE-2024-9380, ggf. mit CVE-2024-8190)

03
Webshell & Credential-Diebstahl – Persistenz und base64-kodierte Skripte zum Auslesen verschlüsselter Admin-Zugangsdaten

04
Ausbreitung & Spurenverwischung – Reverse-TCP-C2, Lateral Movement, Entfernen der Webshells

Betroffenheit & Fixversionen

CSA-Version	Verwundbar bis	Fixversion (Ziel)
CSA 5.0.x	`5.0.1 und älter`	`5.0.2`
CSA 4.6	4.6 (Patch 518 und älter, in Ketten ausgenutzt)	EOL – Migration auf 5.0.2

Betroffen ist die Admin-Web-Konsole der Ivanti CSA in Version **5.0.1 und älter**; behoben in `5.0.2`. Die 4.6-Reihe ist End-of-Life und wurde in den beobachteten Exploit-Ketten ausgenutzt – hier ist die Migration auf 5.0.2 zwingend. Exakte Versionsstände gegen das Hersteller-Advisory abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff über diese Kette 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

Sep 2024
Erste CSA-Zero-Day-Angriffe (CVE-2024-8190 / 8963)

08.10.2024
Ivanti-Advisory für CVE-2024-9379/9380/9381 · Fix 5.0.2

09.10.2024
CISA KEV – aktiv ausgenutzt · Frist 30.10.2024

22.01.2025
CISA/FBI Joint Advisory AA25-022A – Exploit-Ketten & IoCs

Ihr Maßnahmenplan.

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

SOFORT	PARALLEL	DANACH
Auf 5.0.2 patchen / 4.6 migrieren	Threat Hunting / IoC-Abgleich	Zugangsdaten rotieren

01 Betroffenheit feststellen

CSA-Versionsstand prüfen: Ist eine Appliance in 5.0.1 oder älter bzw. in der 4.6-Reihe im Einsatz und aus dem Internet erreichbar? Genau diese Konstellation ist Ziel der aktiven Kampagne.

02 Patchen bzw. migrieren

Auf `CSA 5.0.2` aktualisieren. Die 4.6-Reihe ist End-of-Life und erhält keinen direkten Fix – hier ist die Migration auf 5.0.2 erforderlich.

03 Kompromittierung ausschließen

Da die Lücke seit Oktober 2024 aktiv verkettet ausgenutzt wird, ist ein reines Patchen nicht ausreichend. Web-Verzeichnisse auf hinterlegte Webshells, ungewöhnliche PHP-Dateien und base64-kodierte Skripte prüfen sowie die IoCs aus CISA AA25-022A abgleichen.

04 Zugangsdaten rotieren

Bei Verdacht auf Kompromittierung alle auf der Appliance hinterlegten Administrator- und Dienst-Zugangsdaten als offengelegt behandeln und rotieren – die Angreifer haben nachweislich verschlüsselte Admin-Credentials ausgelesen.

05 Perimeter absichern

Erreichbarkeit der Admin-Konsole aus dem Internet auf das Nötigste einschränken und Zugriffe kontinuierlich überwachen. Die CSA ist als Edge-Gerät ein bevorzugtes Erstzugriffsziel.

Kompromittierungs-Indikatoren (IoCs)

ANGRIFFS-ENDPUNKTE

Konsolen-Skripte wie `DateTimeTab.php` (Command-Injection-Kette) sowie neu abgelegte, unbekannte PHP-Dateien im Web-Verzeichnis

VERHALTENSMARKER

Reverse-TCP-C2-Verbindungen base64-kodierte Python/Shell-Skripte zum Auslesen verschlüsselter Admin-Credentials

VOLLSTÄNDIGE IOCS

IP-Adressen, Datei-Hashes und Webshell-Namen im CISA/FBI-Advisory `AA25-022A`

Zur Einordnung: Die genannten Marker beschreiben das dokumentierte Angreifer-Verhalten aus AA25-022A; die dortige IoC-Liste (IPs, Hashes) ist maßgeblich und flüchtig. Kein Ersatz für die Analyse Ihrer eigenen Web- und Auth-Logs.

Wichtig: Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff. Da die Kette seit Oktober 2024 aktiv ausgenutzt wird und Angreifer Webshells sowie gestohlene Credentials hinterlassen, muss jede exponierte, ungepatchte CSA bis zum Beweis des Gegenteils als potenziell kompromittiert behandelt werden.

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: Neu abgelegte Webshells, anomale ausgehende C2-Verbindungen und Konsolen-Zugriffe ohne vorherige Anmeldung 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-CSA-Appliances 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

- Patch auf CSA 5.0.2 bzw. Migration der 4.6-Reihe sofort anordnen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung; Admin-Zugangsdaten rotieren.
- Über eine dauerhafte Überwachung der internetnahen Edge-Geräte 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-2024-9380 und dem Ivanti CSA-Perimeter.

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

Termin buchen

Quellen: NVD CVE-2024-9380 · Ivanti Security Advisory (CVE-2024-9379/9380/9381, Fix 5.0.2) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 09.10.2024, Frist 30.10.2024) · CISA/FBI Joint Cybersecurity Advisory AA25-022A. Angaben nach bestem Wissen zum Stand 14.07.2026; Versionsstände und IoCs gegen die Hersteller- und CISA-Advisories abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.