AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-9379

SQL-Injection in der Ivanti Cloud Services Appliance.

Ein authentifizierter Angreifer mit Admin-Rechten kann über die Admin-Web-Konsole der Cloud Services Appliance beliebige SQL-Befehle ausführen. In freier Wildbahn wird die Lücke nicht allein, sondern verkettet mit dem Admin-Bypass CVE-2024-8963 ausgenutzt – der Angreifer verschafft sich damit erst den benötigten Admin-Zugang und schreibt anschließend eigene Konten in die Datenbank, um eine Web-Shell aufzubauen.

Geschäftsrisiko: unbefugter Vollzugriff auf ein Perimeter-Gateway – mit Potenzial für Anlage versteckter Admin-Konten, Diebstahl von Zugangsdaten, Lateral Movement ins interne Netz 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, ohne Zutun des Nutzers – aber nur mit bereits vorhandenen Admin-Rechten. Bei Erfolg volle Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. NVD wertet 7,2 (HOCH); Ivanti selbst 6,5 (MITTEL).

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
September 2024	CSA 4.6.x (End-of-Life) + 5.0.1 und älter	Sofort

Das Wichtigste in 60 Sekunden.

7,2 · HOCH
CVSS-Schweregrad (NVD)

SQL-Injection
Admin-Web-Konsole der CSA

Aktiv
ausgenutzt · CISA KEV (09.10.2024)

Nur per Chain
Admin-Zugang meist über CVE-2024-8963

Die Ursache: Die Admin-Web-Konsole der CSA übergibt Eingaben aus dem Konsolen-Formular ungefiltert an die Datenbank (CWE-89). Über das Feld **Lockout Attempts** lässt sich hinter einem gültigen Wert ein zweiter SQL-Befehl anhängen, den die Anwendung mitverarbeitet. So kann ein Angreifer eigene Datensätze in die Tabelle `user_info` schreiben. Der Zugriff setzt Admin-Rechte voraus – in den beobachteten Angriffen liefert der Admin-Bypass `CVE-2024-8963` genau diese Voraussetzung.

ANGRIFFSKETTE

01
Admin-Bypass – über `CVE-2024-8963` (Path Traversal) unautorisierten Admin-Zugang erlangen

02
SQL-Injection – im Feld `Lockout Attempts` ein `INSERT` in die Tabelle `user_info` anhängen

03
Web-Shell bauen – über wiederholte `echo`-Kommandos schrittweise eine persistente Shell aufbauen

04
Zugriff – versteckte Konten, Diebstahl von Zugangsdaten, Discovery-Tools (Obelisk, GoGo) und Lateral Movement

Betroffenheit & Fixversionen

CSA-Version	Verwundbar bis	Fixversion (Ziel)
4.6.x	`Patch 518 und älter – aktiv ausgenutzt`	kein Fix · End-of-Life → auf 5.0.x migrieren
5.0.x	`5.0.1 und älter`	`5.0.2`

CSA 4.6.x ist **End-of-Life** – der letzte Sicherheitsfix erschien am 10.09.2024, danach gibt es keine Patches mehr. Betroffene Systeme müssen auf CSA 5.0.2 (oder neuer) migriert werden; ein Update innerhalb des 4.6-Zweigs ist nicht möglich.

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

10.09.2024
Letzter Sicherheitsfix für CSA 4.6 – danach End-of-Life

September 2024
Erste beobachtete Ausnutzung (u. a. Diebstahl von Admin-Zugangsdaten)

08.10.2024
Ivanti-Advisory zu CVE-2024-9379 / -9380 / -9381; Fix in CSA 5.0.2

09.10.2024
Aufnahme in CISA KEV · Behörden-Frist 30.10.2024

22.01.2025
CISA/FBI-Joint-Advisory AA25-022A mit Details und IoCs

Ihr Maßnahmenplan.

In dieser Reihenfolge – der einzige belastbare Fix ist die Migration auf 5.0.x.

SOFORT	KURZFRISTIG	PARALLEL

01 Betroffenheit feststellen

Version der Cloud Services Appliance ermitteln: Läuft eine 4.6.x (End-of-Life) oder eine 5.0.1 bzw. älter? Ist die Admin-Web-Konsole aus dem Internet erreichbar? Genau diese Konstellation ist das Ziel der beobachteten Angriffe.

02 Exposition reduzieren

Bis zur Migration den Zugriff auf die Admin-Konsole strikt einschränken (nur vertrauenswürdige Management-Netze/VPN, nicht aus dem offenen Internet). Das entschärft zugleich den vorgelagerten Admin-Bypass `CVE-2024-8963`, der die eigentliche Voraussetzung dieser SQL-Injection liefert.

03 Migrieren statt patchen

Es gibt keinen Patch innerhalb von 4.6.x. Auf `CSA 5.0.2` (oder neuer) migrieren. Bei Verdacht auf Kompromittierung empfiehlt Ivanti, das System neu aufzusetzen (Rebuild) statt nur zu aktualisieren.

04 Kompromittierung ausschließen

Auf anomale Anlage von Benutzer-/Admin-Konten prüfen und Web-/Zugriffs-Logs auf die IoCs unten abgleichen – insbesondere Aufrufe von `/client/index.php%3f.php/gsb/broker.php` sowie base64-kodierte Skripte, die eine Web-Shell aufzubauen versuchen. Ein Update schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Verkettete Lücken mitbetrachten

Die Kampagne nutzt `CVE-2024-9379` nie allein, sondern in Ketten mit `CVE-2024-8963` sowie `CVE-2024-8190` / `CVE-2024-9380` (RCE). Alle offenen CSA-CVEs im selben Wartungsfenster schließen und Zugangsdaten nach einem möglichen Vorfall rotieren.

Kompromittierungs-Indikatoren (IoCs)

ANGRIFFS-ENDPUNKTE (GET/POST)

`/client/index.php%3f.php/gsb/broker.php`
`/client/index.php%3f.php/gsb/datetime.php`

SQL-INJECTION-MARKER

`INSERT INTO user_info(...)` im Feld `Lockout Attempts`
base64-kodierte `echo`-Kommandos → Web-Shell

BEOBACHTETE QUELL-IPS

`142.171.217.195` · `154.64.226.166`
`216.131.75.53` · `23.236.66.97`
`38.207.159.76`

Zur Einordnung: Endpunkte und IPs stammen aus dem CISA/FBI-Advisory AA25-022A und sind eine Momentaufnahme der beobachteten Kampagne (September 2024). Einige IPs können auch legitimer Aktivität zugeordnet sein – vor dem Blockieren prüfen. Die Log-Aufrufe sind auffällig vor allem in Verbindung mit anomaler Konten-Anlage; sie ersetzen nicht die Analyse Ihrer eigenen Zugriffs- und Auth-Logs.

Wichtig: Erfolgreiche Ausnutzung setzt Admin-Rechte voraus – die im Feld verkettete Kombination mit dem Admin-Bypass CVE-2024-8963 macht daraus faktisch einen Angriff ohne gültige Zugangsdaten. Ein reines Update ohne Kompromittierungs-Prüfung übersieht bereits angelegte versteckte Konten.

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: Die anomale Anlage von Admin-Konten und base64-kodierte Web-Shell-Versuche auf der CSA fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden aus dem Internet erreichbare, ungepatchte bzw. End-of-Life Ivanti CSA 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

- Migration auf CSA 5.0.2 anordnen; End-of-Life-4.6.x-Systeme außer Betrieb nehmen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – 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-2024-9379 und dem Ivanti CSA-Perimeter.

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

Termin buchen

Quellen: NVD CVE-2024-9379 · Ivanti Security Advisory (CSA CVE-2024-9379 / -9380 / -9381) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 09.10.2024) · CISA/FBI Joint Cybersecurity Advisory AA25-022A (22.01.2025). 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.