AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-8963

Path-Traversal & Admin-Bypass in Ivanti Cloud Services Appliance.

Ein nicht authentifizierter Angreifer aus dem Internet kann über eine Path-Traversal-Lücke die Authentifizierung des CSA-Web-Brokers umgehen und auf geschützte Verwaltungsfunktionen zugreifen. In Verkettung mit der Command-Injection CVE-2024-8190 führt das zu vollständiger Fernübernahme (RCE) – seit September 2024 aktiv ausgenutzt, um Webshells und C2-Implantate abzulegen.

> **Geschäftsrisiko:** vollständige Fernübernahme des Gateways, Diebstahl von Zugangsdaten und ein Brückenkopf ins interne Netz – mit Potenzial für Datenabfluss, Ransomware und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

9,4 / 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:L` – aus dem Netz, ohne Rechte, ohne Zutun – hohe Wirkung auf Vertraulichkeit und Integrität. Ivanti bewertet 9,4; das NVD (NIST) 9,1.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
September 2024	CSA 4.6 vor Patch 519 (4.6.x ist End-of-Life)	Sofort

Das Wichtigste in 60 Sekunden.

9,4 · KRITISCH
CVSS-Schweregrad

Admin-Bypass
geschützte CSA-Endpunkte ohne Login

Aktiv
ausgenutzt · CISA KEV · verkettet mit CVE-2024-8190

Nur 4.6
5.0 nicht betroffen · 4.6 ist EoL

Die Ursache: Der CSA-Web-Broker verarbeitet URLs, bevor er prozentkodierte Zeichen dekodiert. Über ein eingeschobenes `%3F.php` (kodiertes „?") lässt sich ein zulässiger, ungeschützter Pfad voranstellen und dahinter ein eigentlich authentifizierungspflichtiger PHP-Endpunkt anhängen. Der Broker prüft die Zugriffsrechte am sichtbaren Vorderteil, führt aber den geschützten Endpunkt aus – die Authentifizierung wird umgangen. Behoben wurde die Lücke beiläufig mit CSA 4.6 Patch 519.

ANGRIFFSKETTE

01
Broker exponiert – die CSA ist aus dem Internet erreichbar

02
Path Traversal – via `/client/index.php%3F.php/gsb/users.php` geschützte Endpunkte ohne Login erreichen (CVE-2024-8963)

03
Command Injection – über den freigelegten Endpunkt CVE-2024-8190 auslösen und OS-Befehle als root ausführen

04
Persistenz – Webshells ablegen, Zugangsdaten abgreifen, reverse_ssh-C2 nachladen

Betroffenheit & Fixversionen

CSA-Version	Verwundbar bis	Fixversion (Ziel)
CSA 4.6	`< 4.6 Patch 519`	`4.6 Patch 519`
CSA 4.6.x (EoL)	alle Builds vor Patch 519	Migration auf CSA 5.0
CSA 5.0	nicht betroffen	—

CSA 4.6 hat den End-of-Life-Status erreicht: Patch 519 (10.09.2024) ist der letzte Backport für den 4.6-Zweig. Ivanti empfiehlt die Migration auf CSA 5.0. Build-Stand gegen das Hersteller-Advisory abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff oder RCE 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
CSA 4.6 Patch 519 veröffentlicht (behebt CVE-2024-8963 beiläufig)

13.09.2024
Ivanti-Advisory zu CVE-2024-8190 – bereits aktiv ausgenutzt

19.09.2024
Ivanti-Advisory zu CVE-2024-8963 · Aufnahme in CISA KEV

Sep–Okt 2024
Verkettete Ausnutzung, Webshells und reverse_ssh-C2 beobachtet

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

Ihr Maßnahmenplan.

In dieser Reihenfolge – Isolation vor Migration, Migration vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Exposition prüfen & isolieren	Patch 519 / Migration auf 5.0	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

Prüfen, ob eine Ivanti CSA 4.6 im Einsatz und aus dem Internet erreichbar ist. Version und Patch-Stand ermitteln – alles vor `4.6 Patch 519` ist verwundbar. CSA-Broker möglichst vom Internet trennen, bis der Patch- bzw. Migrationsstatus geklärt ist.

02 Patchen bzw. migrieren

Falls noch nicht geschehen, `4.6 Patch 519` einspielen. Da 4.6 End-of-Life ist, ist die Migration auf CSA 5.0 (oder höher) die nachhaltige Lösung – Patch 519 ist der letzte 4.6-Backport.

03 Kompromittierung ausschließen

Aktiv ausgenutzte Systeme gelten bis zum Beweis des Gegenteils als kompromittiert. Auf neu angelegte oder veränderte Admin-Konten, unbekannte Webshells und die IoCs unten prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

04 Bei Verdacht neu aufsetzen

CISA empfiehlt bei Anzeichen einer Kompromittierung, die Appliance vom Netz zu nehmen, forensisch zu sichern und aus vertrauenswürdigem Stand neu aufzusetzen sowie alle darauf genutzten Zugangsdaten zu rotieren.

05 Verkettete CVEs mitbehandeln

Die beobachteten Ketten nutzen CVE-2024-8963 zusammen mit CVE-2024-8190 (Command Injection), CVE-2024-9379 (SQLi) bzw. CVE-2024-9380 (Command Injection). Sicherstellen, dass alle über Patch 519 / 5.0 abgedeckt sind.

Kompromittierungs-Indikatoren (IoCs)

TRAVERSAL-MUSTER (URL)

`/client/index.php%3F.php/gsb/users.php`

Muster: `<Pfad>%3F.php<geschützter Pfad>`

WEBSHELL-PFADE

`/gsb/help.php` · `/gsb/hsh.php`
`/client/RCClient.php` · `/client/LDSupport.php`
`/rc/config.php` · `/gsb/config.php`

C2-INFRASTRUKTUR

`195.133.52.87` · `8.218.239.22`
`156.251.172.80`
`www.vip8025.mom` · `vip8806.mom`

Zur Einordnung: Die Traversal-URLs erscheinen in den Broker-/Webserver-Logs als reguläre PHP-Aufrufe – auffällig durch das eingeschobene %3F.php und Zugriffe auf /gsb/-Endpunkte ohne vorausgehende Anmeldung. IPs, Domains und Webshell-Namen sind eine Momentaufnahme der beobachteten Kampagnen (Quelle: HarfangLab, CISA/FBI AA25-022A) und flüchtig – kein Ersatz für die Analyse Ihrer Logs.

Wichtig: Der Zugriff über die Path-Traversal-Lücke erscheint in den Logs als regulärer PHP-Aufruf – ohne Alarm. Da 4.6 End-of-Life ist, schützt nur die Migration auf 5.0 dauerhaft; ein bloßer Patch auf einer bereits kompromittierten Appliance beseitigt weder Webshells noch abgeflossene Zugangsdaten.

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: Traversal-Aufrufe mit %3F.php und Zugriffe auf /gsb/-Endpunkte 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-4.6-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 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

- Exposition heute prüfen, Patch 519 einspielen bzw. Migration auf CSA 5.0 anstoßen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung; bei Verdacht Appliance neu aufsetzen und Zugangsdaten rotieren.
- Über den weiteren Betrieb einer End-of-Life-Appliance im Perimeter 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-2024-8963 und dem CSA-Perimeter.

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

Termin buchen

Quellen: Ivanti Security Advisory CSA 4.6 (CVE-2024-8963) · NVD NVD-Detail CVE-2024-8963 · CISA Known Exploited Vulnerabilities Catalog · CISA/FBI Joint Advisory AA25-022A · HarfangLab & Censys Threat Reports. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Stände gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.