AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-7593

Authentifizierungs-Bypass im Ivanti vTM Admin-Panel.

Ein nicht authentifizierter Angreifer aus dem Netz kann die fehlerhaft implementierte Authentifizierung des vTM-Admin-Panels umgehen und sich selbst ein Administrator-Konto anlegen – volle Kontrolle über den Load-Balancer, ohne Passwort, ohne Nutzerinteraktion. Die Schwachstelle steht seit September 2024 auf der CISA-KEV-Liste; ein Proof-of-Concept ist öffentlich.

> **Geschäftsrisiko:** vollständige Übernahme des Load-Balancers und damit Kontrolle über den ein- und ausgehenden Anwendungsverkehr – mit Potenzial für Datenabfluss, Umleitung von Traffic, Betriebsunterbrechung 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. Offizieller NVD-Basiswert (CVSS 3.1).

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
24. September 2024 (CISA KEV)	vTM 22.2 – 22.7R1 (außer 22.2R1 · 22.7R2)	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Auth-Bypass
vTM Admin-Panel (Web-UI)

Aktiv
CISA KEV · PoC öffentlich

Admin-Konto
frei wählbar anlegbar

Die Ursache: Die Authentifizierung des vTM-Admin-Panels ist fehlerhaft implementiert (CWE-287 / CWE-303). Der Prüfmechanismus lässt sich umgehen, sodass ein nicht angemeldeter Angreifer eine Verwaltungsanfrage so stellt, als wäre er bereits authentifiziert – und darüber ein **frei wählbares Administrator-Konto** anlegt. Weder Passwort noch gültige Sitzung sind nötig; entscheidend ist allein die Erreichbarkeit der Verwaltungsoberfläche.

ANGRIFFSKETTE

01
Admin-Panel exponiert – die vTM-Verwaltungsoberfläche ist aus dem Netz erreichbar

02
Auth-Prüfung umgehen – die fehlerhafte Authentifizierung lässt eine Verwaltungsanfrage ungeprüft passieren

03
Admin-Konto anlegen – der Angreifer erzeugt ein eigenes Administrator-Konto mit frei gewählten Zugangsdaten

04
Volle Kontrolle – regulärer Admin-Login und Übernahme des Load-Balancers

Betroffenheit & Fixversionen

vTM-Release	Verwundbar bis	Fixversion (Ziel)
22.2	< 22.2R1	22.2R1
22.3	22.3 · 22.3R2 (< 22.3R3)	22.3R3
22.5	22.5R1 (< 22.5R2)	22.5R2
22.6	22.6R1 (< 22.6R2)	22.6R2
22.7	22.7R1 (< 22.7R2)	22.7R2

Nicht betroffen sind bereits 22.2R1 und 22.7R2. Exakte Build-Ranges des eigenen Zweigs gegen das Hersteller-Advisory abgleichen. Ivanti hat die Fixes über die jeweiligen R2-/R3-Releases der Zweige ausgeliefert.

Regulatorischer Hinweis: Ein bestätigter unbefugter administrativer Zugriff 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

13.08.2024
NVD veröffentlicht CVE-2024-7593 · CVSS 9,8

08/2024
Ivanti Security Advisory · Proof-of-Concept öffentlich

24.09.2024
Aufnahme in CISA KEV (Frist 15.10.2024)

Seither
Aktiv ausgenutzt – exponierte Admin-Panels im Visier

Ihr Maßnahmenplan.

In dieser Reihenfolge – Erreichbarkeit einschränken vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Admin-Panel abschotten	Patch einspielen	Konten- & Log-Prüfung

01 Betroffenheit feststellen

vTM-Version je Instanz ermitteln und gegen die Fix-Tabelle abgleichen. Prüfen, ob das Admin-Panel (Web-UI, standardmäßig Port 9090) über das interne Management-Netz hinaus erreichbar ist – besonders aus dem Internet oder aus Produktionsnetzen.

02 Sofort abschotten (vor dem Patch)

Den Zugriff auf die Verwaltungsoberfläche gemäß Ivanti-Empfehlung auf ein dediziertes, internes Management-Netz beschränken. Erreichbarkeit aus dem Internet oder untrusted-Netzen per Firewall/ACL unterbinden, bis der Patch eingespielt ist.

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (`22.2R1` · `22.3R3` · `22.5R2` · `22.6R2` · `22.7R2`). Nach dem Upgrade die tatsächlich laufende Build-Version verifizieren.

04 Kompromittierung ausschließen

Die vTM-Benutzerverwaltung auf unbekannte oder unerwartete Administrator-Konten prüfen und Audit-/Zugriffslogs auf Anlage neuer Konten sowie Admin-Anmeldungen aus fremden Quellen durchsuchen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Bereinigen & härten

Unbefugt angelegte Konten entfernen, Zugangsdaten aller Admin-Konten rotieren und die Beschränkung des Admin-Panels auf das Management-Netz als Dauerzustand festschreiben.

Kompromittierungs-Indikatoren (IoCs)

PRIMÄRER INDIKATOR

Neu angelegte oder unbekannte `Administrator-Konten` in der vTM-Benutzerverwaltung

ADMIN-PANEL-ZUGRIFF

Zugriffe auf die Web-UI (`:9090`) aus dem Internet oder außerhalb des Management-Netzes

LOG-AUFFÄLLIGKEIT

Anlage von Nutzern / Admin-Anmeldungen aus `unerwarteten Quell-IPs` ohne vorausgehende gültige Sitzung

Zur Einordnung: Für diese Schwachstelle liegen keine belastbaren öffentlichen Netzwerk-IoCs (feste IPs/Hostnamen) vor. Die verlässlichste Erkennung ist der Abgleich der Konten-Liste und der Audit-Logs – ein selbst angelegtes Admin-Konto ist der aussagekräftigste Hinweis auf eine Ausnutzung.

Wichtig: Ein erfolgreicher Angriff hinterlässt ein gültiges, vom Angreifer angelegtes Administrator-Konto. Anmeldungen darüber erscheinen anschließend als reguläre Admin-Logins – ohne Alarm. Ohne Prüfung der Konten-Liste und der Audit-Logs bleibt ein bereits erfolgter Zugriff 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: Neu angelegte Administrator-Konten und Admin-Panel-Zugriffe aus fremden Netzen fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden aus dem Netz erreichbare, ungepatchte vTM-Admin-Panels 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 vTM-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 des Admin-Panels heute einschränken, Patch innerhalb der KEV-Logik zeitnah einplanen.
- Prüfen lassen, ob unbefugte Admin-Konten angelegt wurden – dokumentiert für eine etwaige Meldung.
- Beschränkung der Verwaltungsoberfläche auf ein Management-Netz dauerhaft festschreiben.

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-2024-7593 und dem Ivanti vTM-Perimeter.

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

Termin buchen

Quellen: NVD (nvd.nist.gov, CVE-2024-7593, CVSS 3.1 9,8) · Ivanti Security Advisory (Virtual Traffic Manager vTM, CVE-2024-7593) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 24.09.2024). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.