AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-133469

Admin-Zugriff ohne Anmeldung in Xen Orchestra (Virtualisierung).

Xen Orchestra ist die Verwaltungsoberfläche für XCP-ng- und XenServer-Virtualisierung. Ein Angreifer kann sich dort ohne Passwort als Administrator anmelden, indem er ein leeres JSON-Objekt als Anmelde-Token schickt. Von dort aus lassen sich virtuelle Maschinen anlegen und die Hosts bis hin zu Root-Rechten übernehmen. Vates meldet seit dem 10.11.2026 aktive Ausnutzung; die Fixversionen 6.9.2 und 6.10.1 sind verfügbar, die CISA führt die Lücke seit dem 25.11.2026 in ihrem KEV-Katalog.

> **Geschäftsrisiko:** Übernahme der gesamten Virtualisierungsumgebung mit Zugriff auf alle virtuellen Server, Backups und Zugangsdaten, möglicher Ausfall des Rechenzentrumsbetriebs und ein voraussichtlich meldepflichtiger 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 Anmeldung, ohne Mitwirkung eines Nutzers, mit voller Wirkung auf das System. Basiswert laut CNA (GitHub), vom NVD übernommen; die eigene NIST-Bewertung steht noch aus.

AUSNUTZUNG BELEGT SEIT
10.11.2026 (laut Hersteller Vates)

BETROFFEN
Xen Orchestra vor 6.9.2 (stable) und vor 6.10.1 (latest) einschließlich Xen Orchestra Appliance (XOA)

HANDLUNGSBEDARF
Notfall-Change – sofort aktualisieren und vom Internet trennen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Ohne Anmeldung
authenticationToken=j:{} · CWE-287 / CWE-1287

Aktiv ausgenutzt
laut Vates seit 10.11.2026 · CISA KEV seit 25.11.2026

6.9.2 / 6.10.1
Fixversionen stable / latest

Die Ursache: Die REST-Schnittstelle von Xen Orchestra liest das Cookie `authenticationToken` und wandelt den Wert `j:%7B%7D` in ein leeres JSON-Objekt `{}` um. Der Token-Provider prüft nicht, ob tatsächlich eine Zeichenkette übergeben wurde (CWE-1287). Die Token-Datenbank behandelt `{}` als ungefilterte Suche und liefert einfach den ersten gespeicherten Token zurück – **der Angreifer ist damit als dessen Besitzer angemeldet**, solange der Token nicht abgelaufen ist (CWE-287). Über `/rest/v0/users/me/authentication_tokens` holt er sich anschließend wiederverwendbare Login-Token.

ANGRIFFSKETTE

01 **Oberfläche erreichbar** – Xen Orchestra antwortet aus dem Netz

02 **Leerer Token** – Cookie authenticationToken=j:{} meldet den Angreifer als Admin an

03 **Dauerzugang** – Abruf wiederverwendbarer Login-Token über die REST-API

04 **Host-Übernahme** – beobachtet: VM „pivot2“, Code-Ausführung und Root auf XCP-ng-Hosts

Betroffenheit & Fixversionen

Xen-Orchestra-Kanal	Verwundbar bis	Fixversion (Ziel)
Xen Orchestra stable	`vor 6.9.2 (xo-server vor 5.211.2)`	`6.9.2`
Xen Orchestra latest	`vor 6.10.1 (xo-server vor 5.213.1)`	`6.10.1`
Installation aus dem Quellcode	Stände vor PR #10748	`aktueller master`

Angaben laut Vates Security Advisory VSA-2026-062 und NVD. Betroffen sind auch die Xen Orchestra Appliance (XOA) und selbst gebaute Installationen. Vates empfiehlt zusätzlich, Xen Orchestra ausschließlich in einem eigenen Management-Netz zu betreiben. **Bei bestätigter Kompromittierung reicht das Update nicht: alle Zugangsdaten und Geheimnisse rotieren und die betroffenen Systeme neu aufsetzen.**

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf die Virtualisierungsumgebung 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

10.11.2026
Vates VSA-2026-062 · aktive Ausnutzung bestätigt

November 2026
Fixversionen 6.9.2 (stable) und 6.10.1 (latest)

23.11.2026
CVE-2026-133469 veröffentlicht (NVD)

25.11.2026
CISA KEV · Frist für US-Behörden 28.11.2026

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – vom Internet trennen vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Erreichbarkeit einschränken	Update auf 6.9.2 / 6.10.1	Kompromittierung prüfen

01 Betroffenheit feststellen

Alle Xen-Orchestra-Instanzen erfassen, auch XOA-Appliances, Testinstallationen und aus dem Quellcode gebaute Server. Version und Kanal prüfen: betroffen ist stable vor `6.9.2` und latest vor `6.10.1`. Klären, ob die Oberfläche aus dem Internet oder aus Partnernetzen erreichbar ist.

02 Sofort Erreichbarkeit einschränken

Xen Orchestra vom Internet trennen und nur aus einem eigenen Management-Netz erreichbar machen. Die von Vates genannten Angreifer-IPs und Tor-Verkehr blockieren. Eine WAF- oder Reverse-Proxy-Regel gegen das Muster `authenticationToken=j:` hilft als Übergang, lässt sich laut Vates aber mit anderen Schreibweisen umgehen.

03 Patchen

Auf `6.9.2` (stable) bzw. `6.10.1` (latest) aktualisieren; das enthält xo-server `5.211.2` bzw. `5.213.1`. Installationen aus dem Quellcode auf den aktuellen `master` bringen. Danach alle bestehenden Login-Token widerrufen.

04 Kompromittierung ausschließen

In Xen Orchestra nach einer VM namens `pivot2` suchen. Auf den XCP-ng-Hosts nach VMs mit `hvm_serial: file`, nach `pivot2` in `/var/log/xensource.log*` und nach den Dateien `/etc/cron.d/zz-ustar`, `/etc/cron.d/zz-ustar2`, `/.ustar5`, `/.ustar6` und `/etc/ld.so.preload` suchen. Bei Treffern alle Zugangsdaten rotieren und neu aufsetzen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ANGREIFER-IPS (LAUT VATES)

`91.211.251.112`
`193.148.56.72`
`37.221.208.216`
`45.66.35.11`
`64.65.0.120`
`64.65.62.160`
`89.47.51.90`
`92.60.37.247`

AUFFÄLLIGE DATEIEN UND OBJEKTE

VM `pivot2` · `hvm_serial: file`
`/etc/cron.d/zz-ustar*` · `/.ustar5` · `/.ustar6`
`/etc/ld.so.preload`

AUFFÄLLIGE MUSTER

Cookie `authenticationToken=j:%7B%7D` bzw. `j:{}`
Verbindungen zu ustar3rqxgnskzgnwkgpofgtvxevm6cx3lxdbwt4mndtveqyaohid.onion (Port 3333)

Zur Einordnung: Die Indikatoren stammen aus dem Vates-Advisory VSA-2026-062 und sind eine Momentaufnahme. Fehlen sie, ist eine Kompromittierung laut Vates nicht ausgeschlossen.

Wichtig: Wer Xen Orchestra kontrolliert, kontrolliert alle virtuellen Server dahinter. Verwaltungsoberflächen von Virtualisierungsplattformen gehören deshalb nie ins offene Internet.

Bildmotive: KI-generierte Symbolbilder

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

Worauf wir bei dieser Schwachstelle achten: Anmeldung an Xen Orchestra mit leerem authenticationToken oder neue VM „pivot2“. Das setzt voraus, dass die nötigen Logquellen angebunden sind.

Vulnerability & Exposure Management

Wir finden Aus dem Netz erreichbare Xen-Orchestra-Instanzen vor 6.9.2 bzw. 6.10.1 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 Xen Orchestra-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

- Update aller Xen-Orchestra-Instanzen als Notfall-Change anordnen.
- Die Verwaltungsoberfläche dauerhaft in ein eigenes Management-Netz verlegen lassen.
- Eine Prüfung der XCP-ng-Hosts auf Kompromittierung seit November 2026 beauftragen.

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 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-2026-133469 und dem Xen Orchestra-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Vates Security Advisory VSA-2026-062 (10.11.2026, aktiv ausgenutzt, Fix 6.9.2 / 6.10.1, IoCs) · NVD/CVE.org CVE-2026-133469 (CVSS 3.1 Basiswert 9,8 laut CNA GitHub, CWE-287 / CWE-1287, veröffentlicht 23.11.2026) · CISA KEV (aufgenommen 25.11.2026, Frist 28.11.2026) · BleepingComputer (10.11.2026). Stand 25.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.