AKTIV AUSGENUTZT · LAUT GOOGLE THREAT INTELLIGENCE

THREAT INTELLIGENCE BRIEFING

CVE-2026-123890

Anmeldung umgangen über den VMware Directory Service.

vCenter ist die zentrale Verwaltung virtualisierter Rechenzentren. Eine Lücke im VMware Directory Service erlaubt einem Angreifer mit Netzzugang zu vCenter, die Anmeldung zu umgehen und eine Sitzung als Administrator zu erhalten. Broadcom hat am 19.11.2026 Updates veröffentlicht; laut Google Threat Intelligence hat die mutmaßlich chinesische Spionagegruppe ARMORY CASTLE die Lücke bereits Anfang September 2026 als Zero-Day ausgenutzt.

> **Geschäftsrisiko:** Übernahme der gesamten Virtualisierungsverwaltung – mit Zugriff auf alle verwalteten Server und Daten, der Möglichkeit, Systeme abzuschalten oder zu verschlüsseln, und einem 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 Anmeldung, ohne Mitwirkung eines Nutzers, mit voller Wirkung auf das System. Basiswert laut Broadcom (VMSA-2026-0009) und NVD.

AUSGENUTZT SEIT
Anfang September 2026 (Zero-Day, laut Google GTIG)

BETROFFEN
vCenter 9.1.x, 9.0.x, 8.0 und 7.0
VCF 5.x · Telco Cloud Platform / Infrastructure

HANDLUNGSBEDARF
Notfall-Change – sofort patchen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Ohne Anmeldung
VMware Directory Service · CWE-288

Seit Sept. 2026
Ausnutzung laut Google GTIG · nicht in CISA KEV

9.1.1.0200 · 9.0.2.0200 · 8.0 U3m
Fixversionen seit 19.11.2026

Die Ursache: Der **VMware Directory Service (vmdir)** verwaltet in vCenter die Single-Sign-On-Identitäten. Laut Broadcom kann ein Angreifer mit Netzzugang zu vCenter die Anmeldung umgehen (**CWE-288, Authentication Bypass**). Google Threat Intelligence beschreibt den Mechanismus genauer: Über die DCE/RPC-Schnittstelle des Dienstes (Port 2012) lässt sich der Sitzungsschlüssel der SRP-Anmeldung ermitteln, **ohne ein Passwort zu kennen**. Ergebnis ist eine angemeldete Sitzung als `administrator@vsphere.local`. Gemeldet wurde die Lücke von Mandiant.

ANGRIFFSKETTE

01 **Netzzugang** – Angreifer erreicht die RPC-Schnittstelle von vCenter (Port 2012)

02 **Anmeldung umgangen** – SRP-Sitzungsschlüssel wird ohne Passwort ermittelt

03 **Administrator-Sitzung** – Zugriff als administrator@vsphere.local, Abzug der SSO-Datenbank

04 **Dauerhafter Zugang** – neue SSO-Admin-Konten, gefälschte SAML-Token, volle Kontrolle

Betroffenheit & Fixversionen

Produkt · Version	Verwundbar bis	Fixversion (Ziel)
vCenter (VCF / VVF) 9.1	`9.1.x vor 9.1.1.0200`	`9.1.1.0200`
vCenter (VCF / VVF) 9.0	`9.0.x vor 9.0.2.0200`	`9.0.2.0200`
vCenter 8.0	`8.0 vor 8.0 U3m`	`8.0 U3m`
VCF 5.x (vCenter)	`5.x vor 5.2.5`	`5.2.5 (KB88287)`
vCenter 7.0	betroffen	nur mit Extended Support
Telco Cloud Platform / Infrastructure	`TCP 3.0–5.2 · TCI 3.0`	siehe KB463116

Angaben laut Broadcom VMSA-2026-0009. Broadcom nennt **keinen Workaround** und stuft das Update als Notfall-Change ein. ESX ist nicht betroffen. vSphere 6.5 und 6.7 sind laut Broadcom als betroffen anzunehmen. Hinweis: vCenter 8.0 U3m und 9.0.2.0200 blockieren derzeit ein späteres Upgrade auf VCF 9.1.1 (KB 67077).

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf die Virtualisierungsverwaltung 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.

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
Port 2012 abschotten	Update einspielen	Kompromittierung prüfen

01 Betroffenheit feststellen

Version aller vCenter-Instanzen prüfen, auch in VCF, vSphere Foundation und Telco Cloud. Betroffen ist jede Version vor `9.1.1.0200`, `9.0.2.0200`, `8.0 U3m` bzw. VCF `5.2.5`, außerdem vCenter 7.0. Klären, aus welchen Netzen vCenter erreichbar ist.

02 Patchen

vCenter auf `9.1.1.0200`, `9.0.2.0200` bzw. `8.0 U3m` aktualisieren, VCF 5.x auf `5.2.5` (KB88287). Laufende VMs bleiben in Betrieb, die Verwaltung ist kurz nicht verfügbar. Für vCenter 7.0 Broadcom-Support kontaktieren oder migrieren.

03 Risiko bis zum Update senken

Broadcom nennt keinen Workaround. vCenter nur aus einem eigenen Verwaltungsnetz erreichbar machen. Google empfiehlt, Port `2012` per Firewall für alle nicht freigegebenen Adressen zu sperren.

04 Kompromittierung ausschließen

SSO-Konten auf unbekannte Administratoren und Maschinenkonten prüfen, die Datei `/tmp/123` und unerwartete SSH-Aktivierungen über die VAMI-API suchen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Google GTIG: Werkzeug BONESAW unter /tmp/123
YARA-Regel G_Hunting_Utility_BONESAW_2

AUSWERTUNGSQUELLEN

vCenter-SSO- und vmdir-Logs
Firewall-Logs zu Port 2012

AUFFÄLLIGE MUSTER

neue SSO-Admin- oder Maschinenkonten
Kopien von /storage/db/vmware-vmdir/data.mdb · SSH über VAMI aktiviert

Zur Einordnung: Die Indikatoren stammen aus der Google-Analyse vom 19.11.2026 zu einer konkreten Kampagne. Sie sind Ansatzpunkte, kein vollständiger Ausschluss.

Wichtig: vCenter steuert alle virtuellen Server eines Rechenzentrums. Wer die Verwaltung übernimmt, kann Systeme abschalten, kopieren oder verschlüsseln – ohne einen einzigen Server einzeln anzugreifen.

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: Ein neues SSO-Administratorkonto in vCenter. Das setzt voraus, dass die nötigen Logquellen angebunden sind.

Vulnerability & Exposure Management

Wir finden Aus fremden Netzen erreichbare vCenter-Server 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 vCenter-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 vCenter-Instanzen als Notfall-Change anordnen.
- Bestätigen lassen, dass vCenter nur aus einem abgeschotteten Verwaltungsnetz erreichbar ist.
- Eine Prüfung auf Kompromittierung seit September 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-2026-123890 und dem vCenter-Perimeter.

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

Termin buchen

Quellen: Broadcom VMSA-2026-0009 (19.11.2026, Fixversionen, CVSS 9,8) · NVD (19.11.2026, CVSS 3.1 Basiswert 9,8, CWE-288) · Google Threat Intelligence Group, ARMORY CASTLE Exploits vSphere (19.11.2026, Ausnutzung seit Anfang September 2026) · CISA KEV (Stand 19.11.2026: nicht gelistet). Stand 19.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.

Bildmotive: KI-generierte Symbolbilder