THREAT INTELLIGENCE BRIEFING

CVE-2026-123903

Erneut Anmeldung umgangen im VMware Directory Service.

vCenter ist die zentrale Verwaltung virtualisierter Rechenzentren. Eine neue Lücke im VMware Directory Service erlaubt einem Angreifer mit Netzzugang zu vCenter, die Anmeldung zu umgehen und unbefugt auf das System zuzugreifen. Broadcom hat am 24.11.2026 Updates veröffentlicht und stuft sie als Notfall-Change ein. Eine Ausnutzung ist bisher nicht bekannt. Die Lücke ist neu und unabhängig von CVE-2026-123890 aus der Vorwoche.

> **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-2026-0011) und NVD.

AUSNUTZUNG
Nicht bekannt (Stand 26.11.2026)

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

HANDLUNGSBEDARF
Notfall-Change laut Broadcom – vor Ausnutzungsbeginn patchen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Ohne Anmeldung
VMware Directory Service · CWE-287

Nicht bekannt
Ausnutzung · nicht in CISA KEV · kein PoC öffentlich

9.1.2 · 9.0.2.0300 · 8.0 U3m
Fixversionen seit 24.11.2026

Die Ursache: Der **VMware Directory Service (vmdir)** verwaltet in vCenter die Single-Sign-On-Identitäten. Laut Broadcom kann ein Angreifer mit Netzzugang zu vCenter dort die Anmeldung umgehen (**CWE-287, Improper Authentication**) und sich **unbefugt Zugriff auf das System** verschaffen. Technische Details hat Broadcom nicht veröffentlicht. Laut Broadcom-FAQ ist die Lücke **neu und eigenständig** – wer nur das Update aus VMSA-2026-0009 eingespielt hat, ist nicht geschützt. Gemeldet wurde sie unabhängig von Forschern bei Qianxin, depthfirst und ThreatBook.

ANGRIFFSKETTE

01	02	03	04
Netzzugang – Angreifer erreicht vCenter über das Netz	**Anmeldung umgangen** – Fehler im VMware Directory Service	**Unbefugter Zugriff** – Zugang zur Verwaltung ohne gültige Zugangsdaten	**Folgeschaden** – Kontrolle über verwaltete Hosts und virtuelle Server möglich

Betroffenheit & Fixversionen

Produkt · Version	Verwundbar bis	Fixversion (Ziel)
vCenter (VCF / VVF) 9.1	`9.1.x vor 9.1.2`	`9.1.2`
vCenter (VCF / VVF) 9.0	`9.0.x vor 9.0.2.0300`	`9.0.2.0300`
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 KB463501

Angaben laut Broadcom VMSA-2026-0011 vom 24.11.2026. Broadcom nennt **keinen Workaround** und stuft das Update als Notfall-Change ein. Das Update aus VMSA-2026-0009 reicht nicht. vSphere 6.5 und 6.7 sind laut Broadcom als betroffen anzunehmen. Im selben Advisory stehen zwei weitere kritische Lücken in ESX (CVE-2026-123910, CVE-2026-123911).

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
Erreichbarkeit einschränken	Update einspielen	Konten prüfen

01 Betroffenheit feststellen

Version aller vCenter-Instanzen prüfen, auch in VCF, vSphere Foundation und Telco Cloud. Betroffen ist jede Version vor `9.1.2`, `9.0.2.0300`, `8.0 U3m` bzw. VCF `5.2.5`, außerdem vCenter 7.0. Klären, aus welchen Netzen vCenter erreichbar ist.

02 Patchen

vCenter auf `9.1.2`, `9.0.2.0300` 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, abgeschotteten Verwaltungsnetz erreichbar machen und den Zugriff per Firewall auf freigegebene Admin-Systeme begrenzen.

04 Kompromittierung ausschließen

SSO-Konten auf unbekannte Administratoren und Maschinenkonten prüfen, Anmeldungen und vmdir-Logs auf Auffälligkeiten auswerten. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS	AUSWERTUNGSQUELLEN	AUFFÄLLIGE MUSTER
Keine – Broadcom nennt keine, Ausnutzung nicht bekannt	vCenter-SSO- und vmdir-Logs Firewall-Logs zu vCenter	neue SSO-Admin- oder Maschinenkonten Anmeldungen aus unbekannten Netzen

Zur Einordnung: Broadcom veröffentlicht keine technischen Details. Die genannten Muster sind Ansatzpunkte für eine Auswertung, keine bestätigten Signaturen.

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

Prüfung auf Angriffsspuren, 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.
- Prüfen lassen, ob noch vCenter 7.0 ohne Extended Support im Einsatz ist.

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-2026-123903 und dem vCenter-Perimeter.

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

Termin buchen

Quellen: Broadcom VMSA-2026-0011 (24.11.2026, Fixversionen, CVSS 9,8, kein Workaround) · Broadcom FAQ zu VMSA-2026-0011 (Notfall-Change, eigenständig gegenüber CVE-2026-123890) · NVD (26.11.2026, CVSS 3.1 Basiswert 9,8, CWE-287) · CISA KEV (Stand 26.11.2026: nicht gelistet). Stand 26.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.

Bildmotive: KI-generierte Symbolbilder