THREAT INTELLIGENCE BRIEFING

CVE-2026-123911

Code-Ausführung auf dem Host durch Use-after-free im I/O-Filter.

ESX ist der Hypervisor, auf dem die virtuellen Server laufen. Ein zweiter Speicherfehler im I/O-Filter-Dienst erlaubt einem Angreifer mit Netzzugang zum Host, dort Code auszuführen – ohne Anmeldung und ohne Zugriff auf eine virtuelle Maschine. Broadcom hat am 24.11.2026 Updates veröffentlicht und stuft sie als Notfall-Change ein. Eine Ausnutzung ist bisher nicht bekannt.

Geschäftsrisiko: Übernahme des Hypervisors – mit Zugriff auf alle virtuellen Server des Hosts, der Möglichkeit, sie 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
ESX 9.1.x, 9.0.x, 8.0 und 7.0
VCF 5.x · Telco Cloud Platform 5.0 / 5.1

HANDLUNGSBEDARF
Notfall-Change laut Broadcom – vor Ausnutzungsbeginn patchen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Ohne Anmeldung
I/O-Filter-Dienst · CWE-416

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

9.1.2 · 9.0.2.0200 · 8.0 U3m
Fixversionen seit 24.11.2026

Die Ursache: Der **I/O-Filter-Dienst** von ESX (Firewall-Regelsatz `iofiltervp`, Port `9080`) dient der Kommunikation mit vCenter, etwa für Speicher-Filter wie Verschlüsselung oder Caching. Laut Broadcom enthält er einen **Zugriff auf bereits freigegebenen Speicher (CWE-416, Use-after-free)**. Ein Angreifer mit Netzzugang zum Host kann darüber **Code auf dem Host ausführen**; eine virtuelle Maschine braucht er dafür laut Broadcom-FAQ nicht. Gemeldet wurde die Lücke vom DEVCORE Research Team über die Zero Day Initiative.

ANGRIFFSKETTE

01 **Netzzugang** – Angreifer erreicht den I/O-Filter-Dienst des Hosts

02 **Speicherfehler** – präparierte Anfrage nutzt bereits freigegebenen Speicher

03 **Code-Ausführung** – Angreifer führt eigenen Code auf dem ESX-Host aus

04 **Folgeschaden** – Zugriff auf alle virtuellen Server des Hosts, Verschlüsselung möglich

Betroffenheit & Fixversionen

Produkt · Version	Verwundbar bis	Fixversion (Ziel)
ESX (VCF / VVF) 9.1	`9.1.x vor 9.1.2`	`ESXi-9.1.2.0-25946735`
ESX (VCF / VVF) 9.0	`9.0.x vor 9.0.2.0200`	`ESXi-9.0.2.0200-25953133`
ESX 8.0	`8.0 vor 8.0 U3m`	`ESXi80U3m-25926933`
VCF 5.x (ESX)	`5.x vor 5.2.5`	`5.2.5 (KB88287)`
ESX 7.0	betroffen	nur mit Extended Support
Telco Cloud Platform	`TCP 5.0.x · 5.1.x`	siehe KB463501

Angaben laut Broadcom VMSA-2026-0011 vom 24.11.2026. Für ESX 8.0 nennt Broadcom eine **Übergangsmaßnahme (KB463535)**: den I/O-Filter-Dienst per ESX-Firewall nur noch für die vCenter-Adresse freigeben. Laut Broadcom ersetzt das kein Update und kann den Clusterbetrieb beeinträchtigen. Auch die vSAN-Witness-Appliance ist betroffen. Dieselben Fixversionen schließen die erste kritische ESX-Lücke CVE-2026-123910.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf einen Hypervisor 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

24.11.2026
CVE-2026-123911 · Überblick

24.11.2026

26.11.2026
CVE im NVD veröffentlicht

Stand heute
Nicht in CISA KEV · kein PoC

Seite 3: Ihr Maßnahmenplan →

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
Port 9080 einschränken	Hosts aktualisieren	Hosts prüfen

01 Betroffenheit feststellen

Build-Stand aller ESX-Hosts prüfen, auch vSAN-Witness-Appliances und Hosts in VCF und Telco Cloud. Betroffen ist jede Version vor `9.1.2`, `9.0.2.0200`, `8.0 U3m` bzw. VCF `5.2.5`, außerdem ESX 7.0. Klären, aus welchen Netzen die Management-Schnittstellen erreichbar sind.

02 Patchen

Hosts auf `ESXi-9.1.2.0-25946735`, `ESXi-9.0.2.0200-25953133` bzw. `ESXi80U3m-25926933` aktualisieren, VCF 5.x auf `5.2.5`. Der Host startet neu; per vMotion laufen die VMs im Cluster weiter. Für ESX 7.0 Broadcom-Support kontaktieren oder migrieren.

03 Risiko bis zum Update senken

Für ESX 8.0 laut KB463535: `esxcli network firewall ruleset set -r iofiltervp --allowed-all false` und danach nur die vCenter-Adresse freigeben. Management-Netze der Hosts generell vom übrigen Netz trennen.

04 Kompromittierung ausschließen

Host-Logs auf unerwartete Prozesse, neue lokale Konten, aktivierte SSH-Dienste und Verbindungen zu Port 9080 aus fremden Netzen prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Keine – Broadcom nennt keine, Ausnutzung nicht bekannt

AUSWERTUNGSQUELLEN

ESX-Host-Logs (hostd, vmkernel, shell)
Firewall-Logs zu Port 9080

AUFFÄLLIGE MUSTER

Verbindungen zu Port 9080 von anderen Systemen als vCenter
Abstürze oder Neustarts des I/O-Filter-Dienstes, neue lokale Konten

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

Wichtig: Auf einem ESX-Host laufen oft Dutzende Server gleichzeitig. Wer den Hypervisor übernimmt, kann sie alle auf einmal abschalten oder verschlüsseln – ein bekanntes Vorgehen von Ransomware-Gruppen.

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: Zugriffe auf Port 9080 eines Hosts von anderen Systemen als vCenter. Das setzt voraus, dass die nötigen Logquellen angebunden sind.

Vulnerability & Exposure Management

Wir finden ESX-Hosts mit erreichbarer Management-Schnittstelle 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 ESX-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 ESX-Hosts als Notfall-Change anordnen.
- Bestätigen lassen, dass die Management-Netze der Hosts abgeschottet sind.
- Prüfen lassen, ob noch ESX 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-2026-123911 und dem ESX-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) · Broadcom KB463535 (Übergangsmaßnahme ESX 8.0, Regelsatz iofiltervp, Port 9080) · Broadcom FAQ zu VMSA-2026-0011 (Notfall-Change, kein VM-Zugriff nötig) · NVD (26.11.2026, CVSS 3.1 Basiswert 9,8, CWE-416) · 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