AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-76466

Cisco Expressway: Root-Befehle über den Cluster-Datenbankdienst.

Ein nicht authentifizierter Angreifer mit Netzwerkzugang kann auf einem geclusterten Cisco Expressway über den Datenbankdienst beliebige Betriebssystembefehle als root ausführen. Ursache sind persistente Cookies und eine unzureichende Prüfung von Client-Zertifikaten, wenn für das Clustering der TLS Verify Mode aktiv ist. Cisco bewertet die Lücke mit 9,8; seit dem 20.11.2026 führt die CISA sie als aktiv ausgenutzt.

> **Geschäftsrisiko:** vollständige Übernahme des Collaboration-Gateways am Netzwerkrand – mit Zugriff auf Sprach-, Video- und Messaging-Verkehr, Sprungbrett ins interne Netz und Gefahr eines meldepflichtigen Sicherheitsvorfalls 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 Anmeldedaten, ohne Nutzerinteraktion, mit geringer Komplexität – volle Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Wert vom Hersteller Cisco (CNA); NVD übernimmt ihn unverändert.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
20. November 2026	Expressway-C & -E bis X15.5.3 nur im Cluster-Betrieb	Sofort – aktiv ausgenutzt, kein Workaround

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (Cisco)

Root-RCE
über den Cluster-Datenbankdienst

KEV
aktiv ausgenutzt · Frist 23.11.2026

0
Workarounds laut Cisco

Die Ursache: Der Datenbankdienst, über den sich die Knoten eines Expressway-Clusters abgleichen, akzeptiert Anfragen auf Basis persistenter Cookies (CWE-798, hart kodierte Zugangsdaten). Zusätzlich werden Client-Zertifikate nicht ausreichend geprüft, wenn für das Clustering der TLS Verify Mode aktiviert ist. Wer im Besitz dieser Cookies ist und den Dienst erreicht, kann bestimmte RPC-Befehle aufrufen und damit beliebige Betriebssystembefehle als root ausführen.

ANGRIFFSKETTE

01	02	03	04
Cluster erreichbar – Angreifer hat Netzwerkzugang zum Datenbankdienst eines geclusterten Expressway	**Cookie einsetzen** – persistente Cookies werden als gültige Berechtigung akzeptiert	**RPC-Aufruf** – gezielte RPC-Befehle an den Datenbankdienst ohne Anmeldung	**root** – beliebige Betriebssystembefehle; laut F6 Weiterzug auf weitere Cluster-Knoten und ins interne Netz

Betroffenheit & Fixversionen

Expressway-Release	Verwundbar bis	Fixversion (Ziel)
X15	X15.5.3 und älter	X15.5.20
X14 und älter	alle	Migration auf Fix-Release
Einzelgerät (kein Cluster)	nicht betroffen	–

Angreifbar nur, wenn eine verwundbare Version läuft **und** das Gerät in einem Cluster konfiguriert ist; Cisco nennt als Ursache zudem die unzureichende Zertifikatsprüfung bei aktivem TLS Verify Mode für das Clustering. Betroffen sind Expressway-C und Expressway-E, virtuell wie als Appliance. Der Fix ist auch Teil des „Cisco Expressway Series Security Hardening Release: October 2026". Laut Cisco gibt es keinen Workaround.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff kann eine meldepflichtige Verletzung darstellen – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen (Erstmeldung binnen 24 h). Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

21.10.2026
Cisco veröffentlicht Advisory und Fix X15.5.20 (CVSS 9,8, kein Workaround)

18.11.2026
F6 berichtet über erste beobachtete Ausnutzung (Unternehmen in Russland, X15.5.3)

20.11.2026
Aufnahme in CISA KEV · Umsetzungsfrist für US-Behörden 23.11.2026

20.11.2026
Argos-Advisory: sofort patchen und Kompromittierung ausschließen

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – Angriffsfläche schließen, patchen, dann Entwarnung prüfen.

SOFORT	24–72 H	PARALLEL
Cluster-Betrieb prüfen, Zugriff auf Cluster-Dienste beschränken	Auf X15.5.20 aktualisieren	Kompromittierungsprüfung / IoC-Abgleich

01 Betroffenheit feststellen

Alle Expressway-C und -E (virtuell und Appliance) inventarisieren, Release gegen die Tabelle abgleichen und prüfen, ob die Geräte in einem Cluster betrieben werden. Einzelgeräte ohne Cluster sind laut Cisco nicht betroffen.

02 Angriffsfläche reduzieren (kein offizieller Workaround)

Cisco nennt keinen Workaround. Als Härtung empfiehlt F6, die Cluster-Kommunikation auf `TCP 4371–4372` ausschließlich zwischen den vertrauenswürdigen Cluster-Knoten zuzulassen. Das ersetzt den Patch nicht.

03 Patchen

Auf `X15.5.20` aktualisieren; Systeme auf X14 und älter auf ein gepflegtes Release migrieren. Alle Knoten eines Clusters einbeziehen.

04 Kompromittierung ausschließen

Die Geräte auf die IoCs unten prüfen, insbesondere unbekannte Python-Dateien unter `/mnt/harddisk/` und auffällige Erlang-Log-Einträge. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Lateral Movement prüfen

Im beobachteten Angriff folgten Netzwerk-Scans, Zugriffe auf SMB, SQL Server und WinRM sowie das Abgreifen von Zugangsdaten aus GitLab-Repositories. Verbindungen von Expressway-Knoten ins interne Netz auswerten und betroffene Zugangsdaten rotieren.

Kompromittierungs-Indikatoren (IoCs)

ANGREIFER-QUELL-IPS

```
66.179.31[.]32
18.130.47[.]116
```

LOG-EINTRAG (ERLANG.LOG)

```
nodeup,'wombat@127.0.0.1'
```

DATEIPFAD-MUSTER

```
/mnt/harddisk/i{0-9}{4}[a-zA-Z]?/*.py
```

Zur Einordnung: Quelle der IoCs: F6 (Pressemitteilung vom 18.11.2026, in der NVD als Referenz verlinkt); Cisco veröffentlicht keine IoCs. IPs sind eine Momentaufnahme eines einzelnen Vorfalls und flüchtig – kein Ersatz für die Analyse der eigenen Logs.

Wichtig: Cisco nennt keinen Workaround, und das Advisory (Stand v1.0) weist noch keine Ausnutzung aus – die CISA führt die Lücke dennoch seit 20.11.2026 als aktiv ausgenutzt. Der Fix X15.5.20 ist seit 21.10.2026 verfügbar; wer noch nicht gepatcht hat, sollte von einer möglichen Kompromittierung ausgehen und prüfen.

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: Unerwartete Verbindungen auf die Cluster-Ports, neue Python-Dateien auf dem Expressway und ausgehende Scans oder SMB-/WinRM-Zugriffe von Expressway-Knoten. Das setzt voraus, dass die nötigen Logquellen angebunden sind.

Vulnerability & Exposure Management

Wir finden geclusterte, ungepatchte Cisco Expressway-C/-E 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 Cisco-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 geclusterten Expressway-Systeme auf X15.5.20 sofort anordnen – kein Workaround, aktive Ausnutzung.
- Kompromittierungsprüfung beauftragen und dokumentieren – für eine etwaige Meldung nach NIS-2 / DSGVO.
- Collaboration-Gateways am Netzwerkrand künftig dauerhaft überwachen und Cluster-Kommunikation strikt segmentieren.

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-2026-76466 und dem Cisco-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Cisco Security Advisory cisco-sa-vcs-static-cred-hr7EWZ8t (v1.0, 21.10.2026) · NVD CVE-2026-76466 · CISA Known Exploited Vulnerabilities Catalog (Aufnahme 20.11.2026) · F6-Pressemitteilung vom 18.11.2026 (in der NVD referenziert). Angaben nach bestem Wissen zum Stand 20.11.2026; Fixversionen gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.