THREAT INTELLIGENCE BRIEFING

CVE-2026-79614

Codeausführung ohne Anmeldung in Zyxel-Routern und -ONTs.

Ein Speicherfehler in der Bibliothek libclinkc.so erlaubt es einem Angreifer ohne Anmeldung, über eine präparierte HTTP-Anfrage Rechte zu erlangen und möglicherweise Befehle auf dem Gerät auszuführen. Betroffen sind 48 Router-, Glasfaser- und Repeater-Modelle von Zyxel. Zyxel hat am 17.11.2026 Firmware-Updates veröffentlicht; eine Ausnutzung ist bislang nicht bekannt.

Geschäftsrisiko: Übernahme des Internet-Routers eines Standorts oder Homeoffice – mit Mitlesen und Umleiten des Datenverkehrs, Einstieg ins Firmennetz und einem möglicherweise 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 Gerät. Basiswert von Zyxel als CNA, von NVD übernommen.

AUSNUTZUNG
Nicht bekannt (Stand 17.11.2026)

BETROFFEN
48 Zyxel-Modelle: DSL-/Ethernet-CPE, Glasfaser-ONTs, WLAN-Extender

HANDLUNGSBEDARF
Dringend – vor Ausnutzungsbeginn patchen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Ohne Anmeldung
HTTP-Anfrage · CWE-787

Nicht bekannt
Ausnutzung · nicht in CISA KEV

48 Modelle
Firmware-Fix seit 17.11.2026

Die Ursache: In der Bibliothek **libclinkc.so** der Web-Verwaltung steckt ein **Schreibzugriff außerhalb des Speicherbereichs** (**CWE-787**). Laut Zyxel kann ein Angreifer ohne Anmeldung mit einer präparierten HTTP-Anfrage Rechte erlangen und möglicherweise Befehle ausführen. Der WAN-Zugriff auf die Verwaltung ist ab Werk aus; ohne Freigabe muss der Angreifer aus dem lokalen Netz kommen.

ANGRIFFSKETTE

01 **Oberfläche erreichbar** – Web-Verwaltung aus dem LAN oder per WAN-Freigabe ansprechbar

02 **Präparierte Anfrage** – Angreifer sendet eine manipulierte HTTP-Anfrage ohne Anmeldung

03 **Speicherfehler** – libclinkc.so schreibt über den vorgesehenen Bereich hinaus

04 **Befehle auf dem Gerät** – erhöhte Rechte, Kontrolle über Router und Datenverkehr

Betroffenheit & Fixversionen

Modell · Reihe	Verwundbar bis	Fixversion (Ziel)
DX/EX3300, 3301	`bis 5.50(ABVY.8.3)C0`	`5.50(ABVY.8.4)C0`
EX5601-T0 / -T1	`bis 5.70(ACDZ.6.3)C0`	`5.70(ACDZ.6.4)C0`
VMG/EMG …-T50B	`bis 5.50(ABPM.9.11)C0`	`5.50(ABPM.9.12)C0`
Weitere (34)	je Modell (Advisory)	Folgeversion je Modell
WE/WX-Extender (4)	je Modell (Advisory)	Folgeversion je Modell

Laut Zyxel-Advisory vom 17.11.2026 (48 Modelle). Firmware **über Zyxel-Vertrieb oder -Support**; Provider-Sondermodelle aktualisiert der Provider. Kein Workaround genannt.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf einen Router mit Firmendaten 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

25.08.2026
CVE-Nummer reserviert

17.11.2026
Zyxel-Advisory + Fixes

17.11.2026
Veröffentlichung bei NVD

Stand heute
Nicht in KEV, kein PoC

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
WAN-Verwaltung aus	Firmware einspielen	Konfiguration prüfen

01 Betroffenheit feststellen

Zyxel-Router, Glasfaser-ONTs und Repeater an Standorten und im Homeoffice erfassen und Modell plus Firmware mit Tabelle 1 des Zyxel-Advisories abgleichen. Vom Provider gestellte Geräte gesondert notieren.

02 Firmware aktualisieren

Die Fix-Firmware je Modell (z. B. `5.50(ABVY.8.4)C0`) über Zyxel-Vertrieb oder -Support anfordern und einspielen. Bei Provider-Geräten das Update beim Provider einfordern.

03 Risiko bis zum Update senken

Fernverwaltung über WAN abschalten (ab Werk aus) und die Web-Oberfläche nur aus einem Verwaltungsnetz zulassen. Gäste- und IoT-Geräte vom LAN trennen.

04 Kompromittierung ausschließen

Konfiguration auf unbekannte Konten, geänderte DNS-Server, Portweiterleitungen und aktivierte Fernzugänge prüfen. Ein Update schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Keine – Zyxel nennt keine, Ausnutzung nicht bekannt

AUSWERTUNGSQUELLEN

Router-Systemlog und Konfiguration
Firewall-Logs zur Web-Verwaltung

AUFFÄLLIGE MUSTER

Zugriffe auf die Verwaltung von fremden Adressen
geänderte DNS-Server oder Weiterleitungen

Zur Einordnung: Es liegen keine CVE-spezifischen Indikatoren vor. Die genannten Muster sind Ansatzpunkte für eine Auswertung, keine bestätigten Signaturen.

Wichtig: Router und Glasfaser-Modems stehen oft unbeachtet in Filialen und Homeoffices. Wer sie kontrolliert, sieht und lenkt den gesamten Datenverkehr dieses Standorts.

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

24/7-SOC aus München: Ein Verwaltungszugriff auf den Router von einer fremden Adresse fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden Zyxel-Router mit offener Web-Verwaltung 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 Zyxel CPE-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

- Bestandsaufnahme aller Zyxel-Router an Standorten und im Homeoffice anordnen.
- Firmware-Update bzw. Provider-Update mit Termin einfordern.
- Klären lassen, dass keine Router-Verwaltung offen im Internet steht.

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 vollständig 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-2026-79614 und dem Zyxel CPE-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Zyxel Security Advisory vom 17.11.2026 (Modelle, Fix-Firmware, CVSS 9,8) · NVD (CVSS 3.1 Basiswert 9,8) · CISA KEV (Stand 17.11.2026: nicht gelistet). Stand 17.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.