THREAT INTELLIGENCE BRIEFING

CVE-2026-107412

Speicherüberläufe in Gateway und AAA von Citrix NetScaler.

In NetScaler ADC und NetScaler Gateway stecken mehrere Speicherüberläufe, die greifen, wenn das Gerät als Gateway (SSL-VPN, ICA-Proxy, CVPN, RDP-Proxy) oder als AAA-Server arbeitet. Ein Angreifer ohne Anmeldung kann das Gerät so zu Fehlverhalten oder zum Ausfall bringen. Citrix hat die Lücken am 12.11.2026 mit 14.1-73.57 und 13.1-64.39 geschlossen; eine Ausnutzung ist bislang nicht bekannt.

> **Geschäftsrisiko:** Ausfall des Fernzugangs für alle Mitarbeitenden, im schlimmsten Fall Kontrolle über das Gerät am Netzrand – mit Einstieg ins Firmennetz und einem meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

9,5 / 10

KRITISCH
CVSS 4.0 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H` – aus dem Netz, ohne Anmeldung, ohne Mitwirkung eines Nutzers, unter bestimmten Angriffsbedingungen, mit voller Wirkung auf Gerät und Folgesysteme. Basiswert laut Citrix als CNA.

AUSNUTZUNG
Nicht bekannt (Stand 13.11.2026)

BETROFFEN
NetScaler ADC/Gateway 14.1 vor 14.1-73.57
13.1 vor 13.1-64.39 · FIPS/NDcPP

HANDLUNGSBEDARF
Dringend – vor Ausnutzungsbeginn patchen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,5 · KRITISCH
CVSS-Schweregrad

Ohne Anmeldung
Gateway / AAA · CWE-119

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

14.1-73.57 · 13.1-64.39
Fixversionen seit 12.11.2026

Die Ursache: Citrix fasst unter dieser CVE **mehrere Speicherüberläufe** zusammen (**CWE-119**, fehlende Begrenzung von Speicherzugriffen). Sie betreffen Geräte, die als **Gateway** (SSL-VPN, ICA-Proxy, CVPN, RDP-Proxy) oder als **AAA-Server** konfiguriert sind. Präparierte Anfragen ohne Anmeldung können zu unvorhersehbarem Verhalten oder zum Ausfall führen. Die Lücke ist Teil des Sammel-Bulletins CTX697305 mit 28 CVEs; technische Details nennt Citrix nicht.

ANGRIFFSKETTE

01	02	03	04
Gateway erreichbar – VPN- oder AAA-Server steht im Internet	**Präparierte Anfrage** – ohne Anmeldung an den Dienst gesendet	**Speicherüberlauf** – Daten landen außerhalb des Puffers	**Fehlverhalten** – Ausfall des Zugangs oder Eingriff ins Gerät

Betroffenheit & Fixversionen

Produkt · Zweig	Verwundbar bis	Fixversion (Ziel)
ADC / Gateway 14.1	vor 14.1-73.57	14.1-73.57
ADC / Gateway 13.1	vor 13.1-64.39	13.1-64.39
ADC 14.1-FIPS	vor 14.1-73.58	14.1-73.58 FIPS
ADC 13.1-FIPS / NDcPP	vor 13.1-37.293	13.1-37.293

Angaben laut Citrix-Bulletin CTX697305. Citrix nennt **keinen Workaround**. Betroffen sind kundenseitig betriebene Geräte, auch NetScaler-Instanzen in Secure-Private-Access-Hybrid-Umgebungen; Citrix-verwaltete Cloud-Dienste aktualisiert der Hersteller selbst.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf den Fernzugang 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

08.10.2026
CVE-Nummer reserviert

12.11.2026
CTX697305 · Fix 14.1-73.57 / 13.1-64.39

13.11.2026
CVE-Record und NVD veröffentlicht

Stand heute
Nicht in CISA KEV · kein PoC

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
Gateways inventarisieren	Update einspielen	Logs prüfen

01 Betroffenheit feststellen

Build aller NetScaler-Geräte prüfen. Betroffen ist, wer in der Konfiguration `add vpn vserver` oder `add authentication vserver` findet.

02 Patchen

Auf `14.1-73.57` bzw. `13.1-64.39` oder neuer aktualisieren, FIPS/NDcPP auf `14.1-73.58` bzw. `13.1-37.293`.

03 Gesamtes Bulletin mitnehmen

Das Update schließt alle 28 CVEs aus CTX697305, darunter CVE-2026-120868 (9,3) in jeder Standardkonfiguration. Nicht mehr unterstützte Zweige ablösen.

04 Auffälligkeiten prüfen

Logs auf unerwartete Neustarts, Abstürze und ungewöhnliche Anfragen an Gateway und AAA prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Keine – Citrix nennt keine, Ausnutzung nicht bekannt

AUSWERTUNGSQUELLEN

NetScaler-System- und Crash-Logs
Gateway-/AAA-Zugriffslogs

AUFFÄLLIGE MUSTER

unerwartete Neustarts oder Abstürze
ungewöhnliche Anfragen vor der Anmeldung

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

Wichtig: NetScaler Gateway ist bei vielen Unternehmen der zentrale Fernzugang. Frühere NetScaler-Lücken wurden nach Bekanntwerden schnell angegriffen.

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: Unerwartete Neustarts eines Gateways fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden Aus dem Internet erreichbare NetScaler Gateways 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 NetScaler-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 NetScaler-Geräte auf die Fixversionen anordnen.
- Bestätigen lassen, welche Gateways im Internet stehen.
- Über eine dauerhafte Überwachung des Fernzugangs entscheiden.

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-2026-107412 und dem NetScaler-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Citrix-Bulletin CTX697305 (12.11.2026, Fixversionen, CVSS 4.0 9,5) · CVE.org / NVD (13.11.2026) · CISA KEV (Stand 13.11.2026: nicht gelistet). Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.