

# Citrix NetScaler: Zero-Day CVE-2026-88779 wird aktiv ausgenutzt - Advisory und Patch in der Nacht zum 4. Oktober

Stand 07.10.2026 16:56 · Sendung: - · Belegstärke: **bestätigt** · berichtet · **vermutet** · Prozent: 100 = bestätigt, 0 = sicher falsch

## Einordnung

## Wissensstand



Lücke, Builds, KEV-Aufnahme und DoS-Wirkung sind durch Hersteller und Behörden gut belegt. Offen sind die Codeausführung, der Zusammenhang mit CVE-2026-88771, die Täter und die Opfer, vor allem in DACH. Beim Datum von Advisory (3. oder 4. Oktober, je nach Zeitzone) und KEV-Aufnahme (4. oder 5. Oktober) weichen die Quellen voneinander ab.

## 1. Was ist passiert, und warum?

### WISSEN

- Citrix-Bulletin CTX697174: CVE-2026-88779 ist ein „Memory overflow“ mit Denial of Service (CWE-119, CVSS4 8,7) in NetScaler ADC und NetScaler Gateway. Betroffen sind nur Geräte, die als SAML Service Provider oder SAML IdP konfiguriert sind. Veröffentlicht wurde das Bulletin am 3. Oktober 2026 (PST). (100 %) [<https://support.citrix.com/external/article/CTX697174>]
- Der Fehler lässt sich aus der Ferne ohne Anmeldung auslösen. (100 %) [<https://watchtowr.com/intelligence/citrix-netscaler-cve-2026-88779-faq/>]
- Citrix schreibt von „targeted attacks on unmitigated NetScaler deployments which can lead to Denial of Service“. (100 %) [<https://www.securityweek.com/exploitation-of-citrix-netscaler-zero-day-hits-appliances-patched-days-earlier/>]
- Die Angriffe begannen am Freitag, 2. Oktober. Admins meldeten Neustarts von bereits vollständig gepatchten Geräten (14.1-73.37). (100 %) [<https://www.bleepingcomputer.com/news/security/citrix-patches-netscaler-saml-zero-day-exploited-in-attacks/>]
- Laut heise ist der Exploit seit dem Abend des 2. Oktober im Umlauf. (100 %) [<https://www.heise.de/news/NetScaler-Admins-aufgepasst-Zero-Day-verursacht-Crashes-und-Codeausfuehrung-11474971.html>]
- Am 2. Oktober veröffentlichte Citrix Hinweise zu einem „konfigurationsabhängigen“ SAML-Problem, noch ohne CVE. (100 %) [<https://pitscaler.com/>]
- Vorgeschichte: Am 27.09.2026 erschien das Bulletin CTX697096 mit acht CVEs. CVE-2026-88771/-88772 (CVSS4 9,5) wurden als Zero-Days ausgenutzt („PitScaler“) und kamen am 27.09. in den CISA KEV. (100 %) [<https://pitscaler.com/>]
- Kevin Beaumont nennt die Lücke „PitScaler 2“. Er sah Exploit-Versuche gegen gepatchte Honeypots, auf einem davon lief eine heruntergeladene Malware-Binärdatei („Both were patched, so new vuln“). (100 %) [<https://www.bleepingcomputer.com/news/security/citrix-patches-netscaler-saml-zero-day-exploited-in-attacks/>]
- watchTowr hat den Fehler auf dem neuesten Build nachgestellt und hält ihn für einen reinen DoS-Bug. Möglicherweise wurden Geräte absichtlich zum Absturz gebracht, um CVE-2026-88771 schneller ausnutzen zu können. (100 %) [<https://www.securityweek.com/exploitation-of-citrix-netscaler-zero-day-hits-appliances-patched-days-earlier/>]
- Rapid7-Analyst Andrew Galvin: Angreifer verketteten CVE-2026-88779 mit der RCE-Lücke CVE-2026-88771 über „a pre-authentication log-poisoning injection and an unrelated

## SAML-parsing crash“. (100 %)

[<https://www.cybersecuritydive.com/news/citrix-patch-third-exploited-flaw-netscaler/832128/>]

- Gemeldet haben die Lücke laut Citrix Bishop Fox und watchTower. (100 %) [<https://www.helpnetsecurity.com/2026/10/05/cisa-flags-new-exploited-netscaler-flaw-as-attackers-crash-appliances-cve-2026-88779/>]

- Gemeldet von watchTower Labs und Bishop Fox. (100 %)

[<https://thehackernews.com/2026/10/new-netscaler-zero-day-exploited-in.html>]

### NICHT BEKANNT

- Ob CVE-2026-88779 allein Code ausführen kann. Citrix und watchTower sagen „nur DoS“, Beaumont beobachtete Malware. Offen ist auch, ob die Malware über eine Kette mit CVE-2026-88771 oder auf einem anderen Weg aufs Gerät kam.

- Ob der Patch vom 27.09. für CVE-2026-88771 vollständig wirkt

- Ob es sich um eine Umgehung des PitScaler-Patches handelt oder um eine eigenständige neue Lücke

- Wer hinter den Angriffen steht

### WAHRSCHEINLICH (Einschätzung)

- CVE-2026-88779 allein ermöglicht in der Praxis Codeausführung (widersprüchlich: A schätzt Codeausführung allgemein auf 45 % / B die Lücke allein auf 20 %) (20 %) – Citrix sieht nur DoS, und watchTower hat den Fehler nachgestellt und kommt zum selben Ergebnis. Dagegen spricht, dass Citrix die SAML-Lücke CVE-2026-8452 früher auch als DoS eingestuft hatte, bevor sie sich als RCE herausstellte. Ein Admin konnte nicht nachweisen, dass die Shell-Befehle in den Anfragen tatsächlich ausgeführt wurden.

- Auf bereits gepatchten Geräten wurde Code ausgeführt, über eine Kette aus dem Absturz und einer weiteren Schwachstelle (45 %) – Dafür sprechen die Malware auf Beaumonts gepatchtem Honeypot und die Verkettung, die Rapid7 beschreibt. Eine Bestätigung durch Citrix oder eine Behörde fehlt.

- Die Angreifer haben nach dem Patch vom 27.09. gezielt in derselben Gerätefamilie weitergesucht (55 %) – Der Exploit kam fünf Tage nach dem Patch und richtet sich gegen frisch gepatchte Builds. Das passt zu früheren Citrix-Wellen, ein direkter Beleg fehlt aber (A 55 %, B 60 %).

## 2. Was ist die Auswirkung?

### WISSEN

- Wird der Fehler wiederholt ausgelöst, bleibt der Dienst nicht verfügbar. Citrix hat keine Auswirkung auf die Integrität von Kundendaten festgestellt. (100 %)

[<https://thehackernews.com/2026/10/new-netscaler-zero-day-exploited-in.html>]

- Laut Citrix ist die Verfügbarkeit betroffen, die Integrität von Kundendaten nicht. (100 %)

[<https://www.techzine.eu/news/security/144737/citrix-warns-of-an-actively-exploited-dos-vulnerability-in-netscaler/>]

- Mit jedem Versuch stürzt der SAML-Dienst ab, nach dem sechsten Absturz startet das Gerät neu. (100 %) [<https://watchtower.com/intelligence/citrix-netscaler-cve-2026-88779-faq/>]

- Neustart nach dem sechsten Absturz des SAML-Dienstes (Rapid7). (100 %) [<https://www.rapid7.com/blog/post/etr-zero-day-exploitation-of-citrix-netscaler-adc-and-gateway-cve-2026-88771-and-cve-2026-88772/>]

- watchTower: Ein einziger präparierter Request genügt, um ein Gerät vom Netz zu nehmen. (100 %) [<https://www.theregister.com/security/2026/10/05/citrix-netscaler-security-snafus-get-even-worse-amid-more-0-day-reports/5301232/>]

- Die australische ACSC ist am 3. Oktober nach eigener Aussage „aware of impacts to Australian organisations“. (100 %) [<https://pitscaler.com/>]

- Mögliche Folgen laut Sophos: Authentifizierung und Remote Access fallen aus. (100 %)

[<https://www.sophos.com/en-us/blog/citrix-netscaler-vulnerability-cve-2026-88779-in-active-exploitation>]

- Erste Welle (88771/88772): LevelBlue fand Payloads, die privilegierte Konten anlegen, Konfigurationsarchive abziehen und als CSS getarnte Webshells setzen. (100 %)

[<https://thehackernews.com/2026/10/citrix-netscaler-post-exploitation.html>]

- Erste Welle in den Niederlanden: Krankenhäuser (u. a. Amphia, ETZ, Frisius MC) und die Regierung schalteten NetScaler ab. Patienten kamen nicht an ihre Akten, Beamte im Homeoffice konnten sich nicht anmelden. (100 %)

[<https://www.techzine.eu/news/security/144591/new-citrix-vulnerability-affects-hospitals-and-government/>]

#### NICHT BEKANNT

- Wie viele Organisationen über CVE-2026-88779 ausgefallen oder kompromittiert sind
- Ob es in DACH Opfer gibt, vor allem Betreiber aus KRITIS oder Industrie
- Ob über diese Lücke Daten abgeflossen sind
- Ob irgendwo eine OT-Fernwartung betroffen war

#### WAHRSCHEINLICH (Einschätzung)

- Unmittelbar fallen vor allem Remote Access und SSO aus: Homeoffice und Fernwartung über SAML funktionieren zeitweise nicht (70 %) – Das ergibt sich direkt aus dem bestätigten DoS mit Neustart. Admins berichten auf Reddit und bei Born von Reboot-Schleifen, die ACSC bestätigt Auswirkungen in Australien. Konkrete Fälle aus DACH gibt es nicht (A 70 %, B 75 %).
- Gefährlicher als der DoS sind Geräte aus der ersten Welle, die schon kompromittiert sind und trotz Patch eine Backdoor tragen (75 %) – Webshells und Superuser-Konten aus PitScaler sind belegt, und ein Patch entfernt keine Backdoor, die schon auf dem Gerät liegt. Laut Citrix erkennt der IOC-Scan nicht alles. A und B schätzen beide 75 %.
- Einzelne Organisationen bekamen über die Kette mit 88779 neue Webshells oder Backdoors (35 %) – Belegt sind Versuche, Skripte nachzuladen, und ein Honeypot mit Malware. Bestätigte Opfer gibt es dafür bisher nicht.

### 3. Wie lange dauert es digital (Wiederherstellung IT)?

#### WISSEN

- Korrigierte Builds: 14.1-73.41, 13.1-64.28, 14.1-73.41 FIPS, 13.1-37.282 FIPS/NDcPP. Geräte mit dem September-Patch müssen noch einmal aktualisiert werden. (100 %)

[<https://support.citrix.com/external/article/CTX697174>]

- Wer erst kürzlich wegen CVE-2026-88771 bis -88778 gepatcht hat, muss erneut aktualisieren. (100 %) [<https://www.bleepingcomputer.com/news/security/citrix-patches-netscaler-saml-zero-day-exploited-in-attacks/>]
- Die von Citrix verwalteten Cloud-Dienste und Adaptive Authentication sind nicht betroffen. (100 %) [<https://www.sophos.com/en-us/blog/citrix-netscaler-vulnerability-cve-2026-88779-in-active-exploitation>]
- Als Übergangslösung gibt es Signaturen für die Global Deny List (virtual patching). (100 %)
- Empfohlen wird: vor Änderungen Logs und Bundles sichern, das IOC-Skript in NetScaler Console laufen lassen (kann Fehlalarme liefern) und bei Kompromittierung neue Instanzen aufsetzen statt die alten weiterzuverwenden. (100 %) [<https://watchtower.com/intelligence/citrix-netscaler-cve-2026-88779-faq/>]
- Laut Citrix kann der IOC-Scan in der NetScaler Console echte Kompromittierungen übersehen. Citrix empfiehlt erfahrene Forensiker. (100 %)

[<https://docs.netscaler.com/en-us/netscaler-console-service/instance-advisory/ioc.html>]

- Das BSI stuft seine PitScaler-Warnung (2026-289305-1132) mit 3/„Orange“ ein und rät, die Logs bis Anfang September zurück zu prüfen. (100 %) [<https://pitscaler.com/>]
- CISA hat US-Bundesbehörden eine Frist bis zum 7. Oktober gesetzt. (100 %) [<https://www.helpnetsecurity.com/2026/10/05/cisa-flags-new-exploited-netscaler-flaw-as-attackers-crash-appliances-cve-2026-88779/>]

#### NICHT BEKANNT

- Ob das BSI seine Warnung um CVE-2026-88779 ergänzt hat
- Wie lange die Wiederherstellung und die forensische Analyse bei konkreten Opfern gedauert haben
- Wie viele Geräte in DACH noch ungepatcht sind

#### WAHRSCHEINLICH (Einschätzung)

- Ein reiner Patch dauert pro Gerät bzw. HA-Paar Stunden. Ist das Gerät kompromittiert, dauern Forensik, Neuaufbau und Rotation der Zugangsdaten Tage bis Wochen. (70 %) – Das entspricht

der Herstellerempfehlung zum Neuaufbau und den Erfahrungen aus CitrixBleed (2023, 2025) und PitScaler 1. Abgezogene Konfigurationen enthalten Schlüssel und Zugangsdaten, und die müssen alle getauscht werden. A und B schätzen beide 70 %.

#### 4. Ist in der Anlage etwas kaputt, das lange dauert?

##### WISSEN

- Die Lücke betrifft IT-Gateways (NetScaler ADC/Gateway), keine Steuerungen. Citrix nennt als Wirkung Denial of Service ohne Auswirkung auf die Datenintegrität. (100 %)

[<https://support.citrix.com/external/article/CTX697174>]

##### NICHT BEKANNT

- Es ist kein Fall bekannt, in dem über diese Lücke Leittechnik oder Fernwirktechnik beeinträchtigt wurde
- Ob irgendwo OT-Fernwartung über betroffene NetScaler lief und ausfiel
- Ob jemand über kompromittierte Gateways Lateral Movement in OT-Netze betrieben hat
- Wie oft NetScaler in DACH als Zugang zur Fernwartung von OT-Netzen genutzt wird

##### WAHRSCHEINLICH (Einschätzung)

- Physische Schäden an Anlagen durch diese Lücke selbst (5 %) – Betroffen ist der Zugang zum Netz in der IT, nicht die Leittechnik. Für Folgen in der OT bräuchte es ein mehrstufiges Lateral Movement, und dazu gibt es keine Berichte. A hält Schäden für eher unwahrscheinlich, B schätzt 5 %.
- Wo Fernwartung über NetScaler läuft, gibt es indirekte Folgen, weil Dienstleister nicht mehr auf die Anlage kommen oder Verbindungen vorsorglich getrennt werden (40 %) – Citrix-Gateways sind in Industrie und KRITIS als Remote Access verbreitet, konkrete Fälle sind aber nicht belegt. A schätzt 50 %, B 40 %, übernommen ist der niedrigere Wert.

#### 5. Wie viele solcher Ziele gibt es?

##### WISSEN

- Censys zählte am 28.09. weltweit 42.735 Hosts mit NetScaler ADC/Gateway, davon 32 % in den USA und 13 % in Deutschland. Unit 42 kam am 27.09. auf 50.277 potenziell verwundbare Instanzen. Diese Zahlen sagen etwas über die Erreichbarkeit aus, nicht über kompromittierte Geräte. (100 %) [<https://pitscaler.com/>]
- Shadowserver zählt mehr als 20.000 aus dem Internet erreichbare NetScaler-Instanzen. (100 %) [<https://www.cybersecuritydive.com/news/citrix-patch-third-exploited-flaw-netscaler/832128/>]
- Die finnische NCSC-FI zählt „Hunderte“ NetScaler-Instanzen in Finnland. (100 %) [<https://pitscaler.com/>]
- Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Deutschland: 138157 gesamt (DNP3 33367, OMRON FINS 23699, ProConOS 16444, EtherNet/IP 15740) (100 %)

##### NICHT BEKANNT

- Wie viele davon SAML nutzen und damit für CVE-2026-88779 anfällig sind
- Wie viele davon schon gepatcht sind
- Zahlen für Österreich und die Schweiz

##### WAHRSCHEINLICH (Einschätzung)

- In Deutschland sind einige Tausend NetScaler aus dem Internet erreichbar, nur ein Teil davon nutzt SAML (75 %) – Hochgerechnet aus den Censys-Zahlen: 13 % von 42.735 ergibt etwa 5.500. Eine direkte Länderzählung gibt es nicht, und der SAML-Anteil ist unbekannt.

#### 6. Kann das wieder passieren?

##### WISSEN

- CVE-2026-88779 ist laut CISA die sechste ausgenutzte NetScaler-Lücke, die 2026 in den KEV-Katalog aufgenommen wurde. (100 %)

[<https://www.securityweek.com/exploitation-of-citrix-netscaler-zero-day-hits-appliances-patched-days-earlier/>]

- Allein in den zwei Wochen seit dem 27.09. ist das die dritte ausgenutzte NetScaler-Zero-Day-Lücke. (100 %)

[<https://www.cybersecuritydive.com/news/citrix-patch-third-exploited-flaw-netscaler/832128/>]

#### NICHT BEKANNT

- Ob im selben SAML-Code weitere Fehler bekannt sind
- Ob sich CVE-2026-88779, wie früher CVE-2026-8452, später doch als Lücke mit Codeausführung herausstellt

#### WAHRSCHEINLICH (Einschätzung)

- In den nächsten Monaten werden weitere ausgenutzte Lücken in Edge-Geräten wie NetScaler, VPN und Firewalls auftauchen (85 %) – Seit Jahren gibt es wiederkehrende Wellen (2019, 2023, 2025, 2026), allein drei NetScaler-Zero-Days in zwei Wochen. Edge-Geräte sind ein bevorzugter Zugang für Initial Access Broker. Citrix hatte schon CVE-2026-8452 zunächst als DoS eingestuft, bevor sie sich als RCE erwies.

## Lage

Seit dem Abend des 2. Oktober 2026 stürzen NetScaler ADC/Gateway mit SAML-Konfiguration ab, auch Geräte mit dem Notfall-Patch vom 27. September. Citrix hat am 3. Oktober (US-Zeit, in Europa früh am 4. Oktober) das Bulletin CTX697174 veröffentlicht: CVE-2026-88779, CVSS4 8,7, offiziell nur Denial of Service. CISA führt die Lücke als aktiv ausgenutzt, und die Frist für US-Bundesbehörden endet heute, am 7. Oktober. Ob sich damit auch Code ausführen lässt, ist umstritten. watchTowr und Citrix sprechen von einem reinen DoS-Bug. Rapid7 beschreibt laut Cybersecurity Dive eine Verkettung mit der älteren RCE-Lücke CVE-2026-88771, und Kevin Beaumont fand auf einem gepatchten Honeypot nachgeladene Malware. Ein Opfer aus dem DACH-Raum ist bisher nicht namentlich bekannt.

|                     |                                                                                                                                                                                                                                                                                                                |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Angriff             | Ausnutzung einer Speicherlücke im SAML-Teil von NetScaler ADC/Gateway: Der Dienst stürzt ab und das Gerät startet neu. Laut Rapid7 wird die Lücke mit der RCE-Lücke CVE-2026-88771 verkettet, und auf einem gepatchten Honeypot wurde Malware nachgeladen. Ob dabei Code ausgeführt wird, ist nicht bestätigt. |
| Wann / Status       | Exploit seit dem Abend des 02.10.2026 (heise, BleepingComputer). Bulletin CTX697174 am 03.10. (PST) bzw. in Europa am 04.10. frühmorgens, zusammen mit den Patches. KEV-Aufnahme am 04. oder 05.10. (widersprüchlich). CISA-Frist am 07.10. · laufend                                                          |
| Täter               | unbekannt – unbekannt                                                                                                                                                                                                                                                                                          |
| Betreiber / Branche | kein einzelner Betreiber – Betreiber von NetScaler ADC/Gateway mit SAML SP/IdP weltweit · branchenübergreifend (Verwaltung, Gesundheit, KRITIS, Industrie)                                                                                                                                                     |
| Anlage / Alter      | Remote-Access-Gateway / Edge-Gerät in der IT ·                                                                                                                                                                                                                                                                 |
| Region              | weltweit; ACSC bestätigt Auswirkungen in Australien; kein DACH-Opfer namentlich bekannt                                                                                                                                                                                                                        |

## Angriffsvektor

Bekannt: Manipulierte SAML-Authentifizierungsanfragen ohne Anmeldung an Geräte, die aus dem Internet erreichbar und als SAML SP/IdP konfiguriert sind (Citrix/watchTowr). Technische Details werden hier bewusst nicht wiedergegeben.

- Der Absturz ist Teil einer Kette mit der älteren RCE-Lücke CVE-2026-88771 (mittel): Rapid7 (über Cybersecurity Dive) beschreibt die Verkettung, und watchTowr hält es für möglich, dass Abstürze die Ausnutzung von CVE-2026-88771 beschleunigen. Citrix hat das nicht bestätigt.
- Die Lücke wurde von Threat Actors gefunden, die schon PitScaler ausgenutzt hatten, als sie den Patch-Diff per Reverse Engineering analysierten (mittel): Kurz nach Patches wird oft der

Patch-Diff analysiert, und der Abstand von fünf Tagen passt dazu. Belegt ist es nicht.

- Ein Initial Access Broker scannt großflächig, um Remote-Access-Zugänge zu sammeln und zu verkaufen (mittel): Beaumont beschreibt viele Quell-IPs und „Spray and Pray“, das ist typisch für opportunistische Kampagnen.
- Der Absturz dient als Hebel, um Geräte neu zu starten und eine ältere Persistenz oder Webshell wieder zu aktivieren (gering): So vermuten es Nutzer auf Reddit. Vom Hersteller ist das nicht bestätigt und technisch nicht belegt.

## Zeitleiste

27.09.2026 Citrix-Bulletin CTX697096 (8 CVEs). CISA nimmt CVE-2026-88771/-88772 in den KEV-Katalog auf. – **bestätigt** [<https://pitscaler.com/>]

29.09.2026 NCSC-UK und NHS England warnen. Niederländische Stellen, darunter Krankenhäuser und die Regierung, schalten NetScaler ab. – **berichtet**

[<https://borncity.com/blog/2026/10/03/citrix-netscaler-adc-neues-saml-authentifizierungsproblem-3-10-2026/>]

02.10.2026 Citrix-Hinweis zu einem konfigurationsabhängigen SAML-Problem, noch ohne CVE. Ab dem Abend stürzen auch gepatchte Geräte ab. – **berichtet**

[<https://www.bleepingcomputer.com/news/security/citrix-patches-netscaler-saml-zero-day-exploited-in-attacks/>]

03.10.2026 Die ACSC bestätigt Auswirkungen bei australischen Organisationen. Citrix veröffentlicht das Bulletin CTX697174 (PST). – **bestätigt**

[<https://support.citrix.com/external/article/CTX697174>]

04.10.2026 Advisory und Patches in Europa frühmorgens verfügbar (14.1-73.41, 13.1-64.28, FIPS/NDcPP) – **berichtet** [<https://www.heise.de/news/Netscaler-Admins-aufgepasst-Zero-Day-verursacht-Crashes-und-Codeausfuehrung-11474971.html>]

04./05.10.2026 CISA nimmt CVE-2026-88779 in den KEV auf (Datum widersprüchlich) – **berichtet**

[<https://www.helpnetsecurity.com/2026/10/05/cisa-flags-new-exploited-netscaler-flaw-as-attackers-crash-appliances-cve-2026-88779/>]

07.10.2026 Die CISA-Frist für US-Bundesbehörden endet – **bestätigt** [<https://www.helpnetsecurity.com/2026/10/05/cisa-flags-new-exploited-netscaler-flaw-as-attackers-crash-appliances-cve-2026-88779/>]

## Früherer Stand: Erstmeldung (04.10.2026 16:45)

Wissen 44 % · wahrscheinlich 22 % · nicht bekannt 34 %

Seit dem Abend des 2. Oktober 2026 bringen manipulierte SAML-Anfragen NetScaler ADC/Gateway zum Absturz. Das trifft auch Geräte, die den Notfall-Patch vom 27. September (PitScaler, CVE-2026-88771/-88772) schon haben. Citrix hat am 3./4. Oktober das Advisory CTX697174 veröffentlicht (CVE-2026-88779, CVSS4 8,7, Patches 14.1-73.41 und 13.1-64.28) und nennt als Folge Denial of Service. Kevin Beaumont meldet dagegen nachgeladene Malware auf einem bereits gepatchten Honeypot. Ob die Lücke Codeausführung erlaubt, ist offiziell nicht bestätigt. Ein Opfer aus DACH ist bisher nicht namentlich bekannt.

## Früherer Stand: Nach 24 Stunden (05.10.2026 17:14)

Wissen 52 % · wahrscheinlich 20 % · nicht bekannt 28 %

Seit dem Abend des 2. Oktober 2026 wird CVE-2026-88779 in NetScaler ADC/Gateway mit SAML-Konfiguration aktiv ausgenutzt. Betroffen sind auch Geräte, auf denen der Notfall-Patch vom 27. September gegen CVE-2026-88771/-88772 schon eingespielt war. Citrix hat dazu das Advisory CTX697174 (CVSS4 8,7) mit Patches veröffentlicht, die CISA hat die Lücke in den KEV-Katalog aufgenommen. Ob die Lücke Codeausführung erlaubt, ist umstritten: watchTower sieht einen reinen DoS-Bug, Kevin Beaumont hat dagegen auf einem gepatchten Honeypot nachgeladene Malware gefunden, und Administratoren berichten von Shell-Befehlen in SAML-Anfragen. Ein namentlich bekanntes Opfer in DACH gibt es bisher nicht.

Öffentliche Einschätzung von OT-Cyber auf Basis öffentlicher Quellen. Prozent = Einschätzung: 100 % bestätigt, 0 % sicher falsch. Fachliche Einschätzung, keine Schuldzuweisung.