

Citrix NetScaler ADC/Gateway: zwei Zero-Days mit Remote Code Execution aktiv ausgenutzt (CVE-2026-88771, CVE-2026-88772)

Stand 02.10.2026 23:06 · Sendung: - · · Belegstärke: **bestätigt** · berichtet · **vermutet** · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

1. Patchen allein reicht nicht: Wer das Gateway seit Anfang September offen hatte, muss prüfen, ob schon jemand drin war, und alle Zugangsdaten tauschen (CC1 ICS Incident Response).
2. Der Fernzugang ist die Haustür zur Anlage: Ein Remote-Access-Gateway darf nie direkt in die OT führen, sondern nur über Jump Host, Segmentierung und starke Authentifizierung (CC4 Secure Remote Access, CC2 Defensible Architecture).
3. Man muss nicht alles machen, sondern die fünf SANS Critical Controls konsequent: Wer weiß, welche Edge-Geräte er hat, sie überwacht und kritische Lücken zuerst schließt, ist vorbereitet, und mit KI schaffen das auch kleine Teams (CC3, CC5).

Wissensstand

■ Wissen 35 % ■ Wahrscheinlich 18 % ■ Nicht bekannt 47 %

Am fünften Tag nach dem Advisory sind Technik, Zeitleiste, Vorgehen der Angreifer und Patches gut belegt. Offen bleibt, wer konkret kompromittiert wurde, besonders in DACH und in der OT, und was mit den gestohlenen Zugangsdaten noch passiert.

1. Was ist passiert, und warum?

WISSEN

- Citrix hat am 27.09.2026 das Bulletin CTX697096 zu CVE-2026-88771 bis -88778 veröffentlicht. Zwei der Lücken wurden schon vor der Veröffentlichung aktiv ausgenutzt. (100 %) [https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-289305-1032.pdf?__blob=publicationFile&v=4]
- CISA bestätigt weltweite aktive Ausnutzung von CVE-2026-88771 und -88772. Beide ermöglichen jeweils für sich Remote Code Execution. CISA hat beide CVEs am 27.09. in den KEV-Katalog aufgenommen und den Alert am 02.10. aktualisiert. (100 %) [<https://www.cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netscaler-adc-gateway>]
- CVE-2026-88771 beruht auf unzureichender Input-Validierung, CVE-2026-88772 auf einem Speicherüberlauf; beide haben CVSS v4.0 9.5. CVE-2026-88771 betrifft jedes Deployment mit verwundbarem Versionsstand, ohne weitere Vorbedingung. (100 %) [https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-289305-1032.pdf?__blob=publicationFile&v=4]
- CVE-2026-88771 wirkt auch in der Standardkonfiguration und ohne Anmeldung. Einen Workaround gibt es nicht, nur das Upgrade hilft. (100 %) [<https://thecyberexpress.com/citrix-netscaler-cve-2026-88771-cve-2026-88772/>]
- CVE-2026-88772 setzt DTLS voraus, das auf VPN-Virtual-Servern standardmäßig aktiv ist. Die Lücke kann zu RCE oder DoS führen. (100 %) [<https://thehackernews.com/2026/09/warning-two-unpatched-citrix-netscaler.html>]
- Laut Unit 42 gab es ab 21./22.08. Fingerprinting-Scans auf über 100 Systeme, vom 04. bis 24.09. DTLS-Ausnutzung mit dem Ablegen von Webshells und ab 21.09. eine weitere Angriffswelle über Command Injection. (100 %) [<https://unit42.paloaltonetworks.com/netscaler-zero-days-exploited/>]

- Laut BSI, das sich auf eSentire beruft, reicht die Ausnutzung mindestens bis zum 05.09.2026 zurück. (100 %) [https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-289305-1032.pdf?__blob=publicationFile&v=4]

- Mandiant/GTIG ordnet die frühen, gezielten Angriffe „advanced and suspected state-sponsored threat actors“ mit mutmaßlichem Spionageziel zu. (100 %)

[<https://www.securityweek.com/government-finance-orgs-targeted-in-weeks-long-netcaler-zero-day-attacks/>]

- watchTowr hat eine Root-Cause-Analyse und einen funktionierenden Proof of Concept veröffentlicht. Innerhalb von Minuten folgten Ausnutzungsversuche, daraus wurde breite „spray and pray“-Massenausnutzung. (100 %) [<https://www.helpnetsecurity.com/2026/09/29/netcaler-zero-day-exploitation-escalates-into-mass-attacks-cve-2026-88771/>]

- Das BSI warnte am 28.09. mit der höchsten Stufe 3 („sehr hoch“) und aktualisierte die Warnung am 01.10. (Version 1.1). (100 %)

[<https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-289305-1032.html>]

- Das BSI bewertet die Ausnutzung als simpel. Durch KI-gestützte Exploit-Entwicklung würden Patches immer schneller analysiert. (100 %) [https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-289305-1032.pdf?__blob=publicationFile&v=4]

NICHT BEKANNT

- Welcher Threat Actor konkret dahintersteckt: GTIG und die Behörden nennen weder eine Gruppe noch einen Staat.

- Wie die Angreifer die Lücken vor Citrix entdeckt haben.

- Ob in DACH gezielt Versorger angegriffen wurden.

- Ob auch CVE-2026-88773 bis -88778 schon ausgenutzt werden; bisher gibt es dazu keine Erkenntnisse.

WAHRSCHEINLICH (Einschätzung)

- Am Anfang standen gezielt vorgehende Spionageakteure. Seit dem PoC nutzen mehrere unabhängige Gruppen die Lücken opportunistisch aus, auch kriminelle. (85 %) – Mandiant spricht von staatsnah/Spionage, Arctic Wolf von „spray and pray“-Folgeangriffen; der PoC ist öffentlich, das BSI nennt die Ausnutzung simpel, GreyNoise und Censys sehen Massenscans. Die Welle passt zeitlich zur PoC-Veröffentlichung.

- Edge-Geräte wie NetScaler sind bevorzugte Ziele, weil sie direkt am Internet hängen und kaum mit EDR überwacht werden. (80 %) – Dasselbe Muster gab es bei Citrix Bleed 2023, CitrixBleed 2 2025 und CVE-2026-3055 im März 2026.

- Auch die übrigen sechs CVEs rücken bald in den Fokus der Angreifer. (55 %) – So schätzt es das BSI ein; Patch-Diffing mit KI-Unterstützung beschleunigt das.

2. Was ist die Auswirkung?

WISSEN

- Laut GTIG erlangten die Angreifer Root-Rechte und setzten die neuen Malware-Familien WHIPSHOT (Webshell) und SLAPSHOT (Tunneling-Tool) ein. In einigen Fällen kam es zu Lateral Movement ins interne Netz. (100 %) [<https://cloud.google.com/blog/topics/threat-intelligence/defending-against-advanced-exploitation-of-citrix-netcaler-adc-and-gateway-appliances/>]

- Mandiant meldet Dutzende betroffene Organisationen in Nordamerika und Europa, mit dem Ziel Aufklärung, Diebstahl von Zugangsdaten und Lateral Movement. Genannt werden Regierung, Finanzwesen, Bildung, Telekommunikation sowie der Rechts- und Beratungssektor. (100 %) [<https://www.securityweek.com/government-finance-orgs-targeted-in-weeks-long-netcaler-zero-day-attacks/>]

- Rapid7 beobachtete, wie die Konfiguration samt verschlüsselter Admin-, LDAP- und RADIUS-Zugangsdaten, Zertifikaten und privaten Schlüsseln abgegriffen wurde. Zwei Kunden waren bestätigt kompromittiert. (100 %) [<https://www.rapid7.com/blog/post/etr-zero-day-exploitation-of-citrix-netcaler-adc-and-gateway-cve-2026-88771-and-cve-2026-88772/>]

- Arctic Wolf zählt mindestens 78 angegriffene Organisationen in den USA, Kanada und Europa, unter anderem aus Energie, Gesundheit, Finanzen, Kommunalverwaltung, Medien und Bildung. (100 %) [<https://arcticwolf.com/resources/blog/critical-citrix-netcaler-adc-and-citrix-netcaler-gateway-vulnerabilities/>]

- Laut LevelBlue (01.10.) legen die Angreifer privilegierte Konten an, leiten NetScaler-Konfigurationsarchive aus und verstecken Webshells. Der Zugang kann dadurch auch nach dem Patch bestehen bleiben. (100 %)

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

- In Rheinland-Pfalz schalteten die Rechenzentren am 27.09. vorsorglich Systeme ab. Gestört waren alle 194 Kommunalverwaltungen (Meldewesen, Pässe, Kfz-Zulassung, Standesamt u. a.). Offiziell heißt es ausdrücklich, es habe „kein erfolgreicher Cyberangriff“ stattgefunden. (100 %)

[<https://www.heise.de/news/IT-Stoerung-trifft-Kommunalverwaltungen-in-Rheinland-Pfalz-11469044.html>]

- Die Südwestfalen-IT schaltete NetScaler am 27.09. ab. Damit fielen bei 72 Kommunen Homeoffice und Einwahl weg. (100 %)

[<https://borncity.com/blog/2026/09/28/rheinland-pfalz-landesweite-software-stoerung-citrix-problem-die-ursache/>]

- In den Niederlanden nahmen Krankenhäuser wie Amphia und Frisius MC nach Warnungen von Z-CERT und NCSC ihre Patientenportale vom Netz. (100 %)

[<https://nos.nl/artikel/2632818-problemen-bij-ziekenhuizen-met-citrix-patienten-kunnen-dossier-niet-inzien>]

NICHT BEKANNT

- Ob es in DACH bestätigte Kompromittierungen gibt, besonders bei Versorgern oder in der Industrie.
- Ob Angreifer über ein Gateway OT-Netze oder Fernwartungszugänge erreicht haben; dazu gibt es keine öffentliche Meldung.
- Welche Daten abgefließen sind und wie viele gestohlene Zugangsdaten im Umlauf sind.

WAHRSCHEINLICH (Einschätzung)

- Die Ausfälle in DACH gehen bisher auf vorsorgliche Abschaltungen zurück. Eingeschränkt waren Homeoffice und externer Zugang, nicht die Versorgung. (78 %) – Die belegten Fälle (RLP, SIT) sind Abschaltungen, die RLP-Behörden dementieren einen Angriff, und Berichte über Versorgungsstörungen gibt es nicht.
- Gestohlene Zugangsdaten und Konfigurationen werden noch Wochen bis Monate nach dem Patch für Folgeangriffe genutzt, auch über Initial Access Broker. (70 %) – Rapid7 und LevelBlue belegen den Abfluss, Mandiant warnt ausdrücklich davor. Nach Citrix Bleed 2023 folgte Ransomware (LockBit).
- Unter den Kompromittierten sind auch DACH-Energieversorger. (30 %) – Arctic Wolf nennt Energie als Sektor und Deutschland stellt rund 13 % der exponierten Hosts, aber es gibt keinen öffentlichen Einzelbeleg.

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

WISSEN

- Behoben ist die Lücke in 14.1-73.37, 13.1-64.23, 14.1-73.37 FIPS und 13.1-37.279 FIPS/NDcPP sowie in neueren Versionen; ältere Builds sind verwundbar. (100 %)

[<https://socprime.com/blog/cve-2026-88771-and-cve-2026-88772-analysis/>]

- Laut BSI reicht Patchen allein nicht, weil Webshells und Konfigurationsänderungen aktiv bleiben können. Logs sollen mindestens ab Anfang September 2026 geprüft werden. (100 %) [https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-289305-1032.pdf?__blob=publicationFile&v=4]

- CISA rät, vor dem Patchen auf Kompromittierung zu prüfen und forensische Spuren zu sichern. (100 %) [<https://www.cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netscaler-adc-gateway>]

- Mandiant (Carmakal): „Upgrading alone will not eradicate post-exploitation access or address stolen credentials“. Empfohlen werden Isolation, das Abschalten von DTLS und die Rotation der Zugangsdaten. (100 %)

[<https://www.cybersecuritydive.com/news/exploitation-citrix-netscaler-what-we-know/831780/>]

- GTIG empfiehlt, Sessions zu widerrufen, Admin-Zugangsdaten, SSH-Keys, TLS-Zertifikate sowie LDAP-, RADIUS- und TACACS-Secrets zu rotieren und nachgelagerte Systeme zu prüfen. (100 %) [<https://cloud.google.com/blog/topics/threat-intelligence/defending-against-active-exploitation-of-citrix-netscaler-adc-and-gateway-appliances/>]

- CVE-2026-88778 wird nicht allein durch das Upgrade behoben; zusätzlich muss Enhanced ISN Generation aktiviert werden. (100 %)

[<https://aicybr.com/blog/citrix-netscaler-cve-2026-88771-88772-zero-day-rce>]

- Laut Kevin Beaumont waren anfangs weniger als 10 % der exponierten Hosts gepatcht. (100 %)

[<https://www.helpnetsecurity.com/2026/09/29/netscaler-zero-day-exploitation-escalates-into-mass-attacks-cve-2026-88771/>]

- In Rheinland-Pfalz wurde der Normalbetrieb ab Dienstag, 29.09., erwartet (widersprüchlich: A Normalbetrieb ab 29.09. / B vollständig bis 30.09., erste Städte meldeten das Ende der Störung). (100 %) [<https://www.heise.de/news/IT-Stoerung-trifft-Kommunalverwaltungen-in-Rheinland-Pfalz-11469044.html>]

- Erste Städte in Rheinland-Pfalz meldeten das Ende der Störung; bis 30.09. sollte der Betrieb wieder vollständig laufen. (100 %) [https://www.rheinpfalz.de/rheinland-pfalz_artikel,-it-sicherheitsl%C3%BCcke-erste-st%C3%A4dte-melden-ende-der-st%C3%B6rung-_arid,5933974.html]

NICHT BEKANNT

- Wie viele Betreiber kompromittiert sind und deshalb eine volle Incident Response brauchen.
- Wie viele Betreiber eine Compromise Assessment gemacht und nicht nur gepatcht haben.
- Ob im Netz hinter den Gateways schon Lateral Movement stattgefunden hat.
- Ob die IOC-Listen vollständig sind; Citrix ergänzt sie laufend.

WAHRSCHEINLICH (Einschätzung)

- Nicht kompromittierte Betreiber sind nach Patch und Prüfung in Stunden bis wenigen Tagen wieder online. (75 %) – Rheinland-Pfalz war nach rund zwei bis drei Tagen wieder in Betrieb; die Angaben zum genauen Tag unterscheiden sich leicht.
- Kompromittierte Betreiber mit Lateral Movement brauchen Wochen für Neuaufbau, Rotation aller Secrets und die Prüfung des internen Netzes. (72 %) – So lief es nach Citrix Bleed 2023, und GTIG empfiehlt einen großen Rotationsumfang.

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

WISSEN

- Die bekannten Angriffe zielen auf Spionage, den Diebstahl von Zugangsdaten und Lateral Movement in IT-Netze. Sabotage, physische Schäden oder Eingriffe in Steuerungen sind nicht berichtet. (100 %) [<https://www.helpnetsecurity.com/2026/09/30/cve-2026-88772-netscaler-exploitation-zero-day/>]

NICHT BEKANNT

- Ob irgendwo ein NetScaler als Remote Access in OT-Netze genutzt wurde und Angreifer dort waren.
- Ob Fernwartungszugänge für Leittechnik betroffen sind.
- Ob physische Anlagen betroffen sind; dazu gibt es keinerlei Meldungen.

WAHRSCHEINLICH (Einschätzung)

- In Anlagen ist bisher nichts physisch beschädigt. (85 %) – Das beobachtete Ziel war Spionage, nicht Sabotage. Es gibt keine Meldungen von Behörden oder Betreibern, und die Ausfälle stammen von Abschaltungen.
- Wo Fernwartung über NetScaler läuft, ist sie während der Abschaltung eingeschränkt, und Techniker müssen vor Ort arbeiten. (65 %) – Bei der SIT ist der Wegfall von Remote Access belegt. Das lässt sich auf Versorger übertragen, ist aber für keinen einzelnen Versorger belegt.
- Wo das Gateway direkt in die OT-Fernwartung führt, ist das Risiko für Folgeangriffe erhöht. (60 %) – In der Branche dient NetScaler oft als zentrales Remote-Access-Gateway, nicht immer mit Jump Host und Segmentierung.

5. Wie viele solcher Ziele gibt es?

WISSEN

- Unit 42/Cortex Xpanse zählte am 27.09. 50.277 exponierte, potenziell verwundbare Instanzen. (100 %) [<https://unit42.paloaltonetworks.com/netscaler-zero-days-exploited/>]
- Censys zählt rund 42.000 aus dem Internet erreichbare NetScaler-Hosts: USA 32 %, Deutschland 13 %, Schweiz, Niederlande und Großbritannien je rund 4 %. (100 %) [<https://www.help>]

- Shadowserver zählt über 23.000 exponierte IPs weltweit, davon rund 3.000 in Deutschland. (100 %) [<https://cybernews.com/security/citrix-netscaler-rce-vulnerabilities-active-attack/>]
- Das BSI spricht, gestützt auf Shadowserver, von mehreren Tausend betroffenen Citrix-Appliances allein in Deutschland. (100 %) [https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-289305-1032.pdf?__blob=publicationFile&v=4]
- Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Deutschland: 137383 gesamt (DNP3 32856, OMRON FINS 23377, ProConOS 16329, EtherNet/IP 15681) (100 %)

NICHT BEKANNT

- Wie viele davon bei Stadtwerken, Versorgern oder in der Industrie stehen; eine Branchenaufschlüsselung ist nicht öffentlich.
- Wie viele inzwischen gepatcht und geprüft sind; die Angabe „unter 10 %“ stammt von einem frühen Stand.
- Die Zahlen widersprechen sich (23.000 / 42.000 / 50.277), weil die Zählmethoden verschieden sind.

WAHRSCHEINLICH (Einschätzung)

- In Deutschland stehen einige Tausend exponierte NetScaler (widersprüchlich: A rund 5.000 als Hochrechnung aus 13 % von 42.000 / B rund 3.000 laut Shadowserver). Ein relevanter Teil, vermutlich Dutzende, gehört KRITIS-nahen Betreibern, Versorgern und Industrie. (60 %) – Die Gesamtzahl ist von BSI und Shadowserver gedeckt; der Branchenanteil ist nur aus der bekannten Verbreitung bei Stadtwerken und Kommunen abgeleitet.

6. Kann das wieder passieren?

WISSEN

- Laut BSI wurden NetScaler-Lücken schon früher genutzt, um in interne Netze einzudringen. Durch KI-gestützte Exploit-Entwicklung werde sich das Tempo erhöhen. (100 %) [https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-289305-1032.pdf?__blob=publicationFile&v=4]
- Schon im März 2026 wurde mit CVE-2026-3055 (CVSS 9.3) eine NetScaler-Lücke angegriffen. (100 %)

[<https://borncity.com/blog/2026/03/30/schwachstelle-cve-2026-3055-in-citrix-netscaler-adc-und-gateway-wird-angegriffen/>]

NICHT BEKANNT

- Ob es weitere, noch unbekannte Lücken gibt.
- Ob die übrigen sechs CVEs dieses Advisories bald ausgenutzt werden.

WAHRSCHEINLICH (Einschätzung)

- In den nächsten 12 Monaten werden weitere kritische Lücken in Edge-Geräten (Citrix, Ivanti, Fortinet usw.) aktiv ausgenutzt. (90 %) – Seit 2019 wiederholt sich das Muster mehrmals pro Jahr, und das BSI erwartet durch KI ein höheres Tempo.

Lage

Citrix hat am 27.09.2026 acht Schwachstellen in NetScaler ADC und Gateway veröffentlicht (CVE-2026-88771 bis -88778). Zwei davon erlauben Remote Code Execution ohne Anmeldung (CVSS v4.0 9.5) und wurden schon Wochen vorher als Zero-Day ausgenutzt, laut Mandiant zuerst von mutmaßlich staatsnahen Akteuren mit Spionageziel und seit dem öffentlichen Proof of Concept auch massenhaft. In Deutschland gibt es bisher vor allem Ausfälle durch vorsorgliche Abschaltungen (Kommunen in Rheinland-Pfalz und NRW); ein Einbruch bei einem DACH-Versorger ist öffentlich nicht belegt.

Angriff

Ausnutzung zweier Pre-Auth-RCE-Zero-Days in NetScaler ADC/Gateway mit Root-Rechten, Webshells (WHIPSHOT), Tunneling (SLAPSHOT), Diebstahl von Zugangsdaten, Zertifikaten und Konfigurationen, angelegten privilegierten Konten und teils Lateral Movement; seit dem PoC Massenausnutzung

Wann / Status	Scans ab 21./22.08.2026, Ausnutzung ab 04.09.2026 (Unit 42; laut BSI/eSentire mindestens ab 05.09.), weitere Welle ab 21.09., Massenausnutzung ab etwa 27.–29.09.2026 · laufend
Täter	Zu Beginn mutmaßlich staatsnahe Spionageakteure (Mandiant/GTIG), danach breite opportunistische Akteure, auch kriminelle; keine Gruppe und kein Staat offiziell benannt – vermutet
Betreiber / Branche	kein einzelner Betreiber – weltweite Kampagne gegen NetScaler-Betreiber · Behörden, Kommunen, Energie, Gesundheit, Finanzen, Telekommunikation, Bildung, Medien, Rechts- und Beratungssektor
Anlage / Alter	Remote-Access-/VPN-Gateway (Edge-Gerät), oft für Fernwartung ·
Region	weltweit, Schwerpunkte Nordamerika und Europa; DACH (Deutschland rund 13 % der exponierten Hosts, Schweiz rund 4 %)
Auswirkungen	Versorgungsausfälle bei Strom, Wasser oder Wärme sind nicht bekannt. Für die Bevölkerung waren bisher vor allem Bürgerdienste spürbar, weil Systeme vorsorglich abgeschaltet wurden: In Rheinland-Pfalz fielen Meldewesen, Pässe, Kfz-Zulassung und Standesamt aus, in 72 Kommunen in NRW Homeoffice und Einwahl, in den Niederlanden Patientenportale von Krankenhäusern. Bei Versorgern kann die Fernwartung eingeschränkt sein, das ist aber nicht einzeln belegt.
Behörden	CISA (USA, KEV-Aufnahme), BSI (Warnstufe 3, Version 1.1), NCSC und Z-CERT (Niederlande); dazu Threat-Intelligence-Teams von Mandiant/GTIG, Unit 42, Rapid7, Arctic Wolf, LevelBlue, eSentire, watchTower, Censys, Shadowserver und GreyNoise.
Regulatorik	Betreiber kritischer Anlagen und NIS2-pflichtige Einrichtungen müssen erhebliche Sicherheitsvorfälle an das BSI melden. Ob es in diesem Fall Meldungen gab, ist nicht öffentlich. Die vorsorglichen Abschaltungen in RLP wurden ausdrücklich nicht als erfolgreicher Angriff eingestuft.

Angriffsvektor

Bekannt: Ausnutzung der Pre-Auth-Lücken CVE-2026-88771 (Input-Validierung, Standardkonfiguration) und CVE-2026-88772 (Speicherüberlauf, DTLS) an internetexponierten NetScaler-Gateways

- Hypothese: Folgeangriffe auf die interne IT und OT mit am Gateway gestohlenen Zugangsdaten (Admin-, LDAP-, RADIUS-Konten, Sessions, Zertifikate) (hoch): Rapid7, LevelBlue und Mandiant belegen, dass Konfigurationen und Zugangsdaten abgegriffen wurden; Mandiant warnt, dass das Upgrade gestohlene Zugangsdaten nicht unschädlich macht.
- Hypothese: Weiterverkauf der erlangten Zugänge über Initial Access Broker an Ransomware-Gruppen (mittel): Nach Citrix Bleed 2023 folgte Ransomware (LockBit), und seit dem PoC sind auch kriminelle Akteure beteiligt.
- Hypothese: Missbrauch von Fernwartungszugängen über das Gateway in OT-Netze, wo kein Jump Host und keine Segmentierung dazwischen liegt (mittel): NetScaler ist bei Versorgern oft zentrales Remote-Access-Gateway, aber ein solcher Fall ist öffentlich nicht belegt.
- Hypothese: Ausnutzung der übrigen CVEs dieses Advisories (-88773 bis -88778) bei unvollständig gepatchten Systemen, etwa ohne aktivierte Enhanced ISN Generation bei -88778 (gering): Das BSI erwartet, dass KI-gestütztes Patch-Diffing schneller wird, bisher gibt es aber keine Erkenntnisse zur Ausnutzung.

Zeitleiste

21./22.08.2026 Erste Fingerprinting-Scans auf über 100 NetScaler-Systeme – [berichtet](#)

[<https://unit42.paloaltonetworks.com/netscaler-zero-days-exploited/>]

04.09.2026 Beginn der DTLS-Ausnutzung mit Webshells (bis 24.09.) – **berichtet**

[<https://unit42.paloaltonetworks.com/netscaler-zero-days-exploited/>]

spätestens 05.09.2026 Ausnutzung reicht laut BSI (unter Berufung auf eSentire) mindestens bis hierher zurück – **bestätigt** [https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-289305-1032.pdf?__blob=publicationFile&v=4]

ab 21.09.2026 Weitere Angriffswelle über Command Injection – **berichtet**

[<https://unit42.paloaltonetworks.com/netscaler-zero-days-exploited/>]

27.09.2026 Citrix veröffentlicht Bulletin CTX697096 (CVE-2026-88771 bis -88778) – **bestätigt** [https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-289305-1032.pdf?__blob=publicationFile&v=4]

27.09.2026 CISA-Alert und Aufnahme beider CVEs in den KEV-Katalog – **bestätigt** [<https://www.cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netscaler-adc-gateway>]

27.09.2026 Vorsorgliche Abschaltungen: Rechenzentren in Rheinland-Pfalz (194 Kommunalverwaltungen) und Südwestfalen-IT (72 Kommunen) – **berichtet**

[<https://borncity.com/blog/2026/09/28/rheinland-pfalz-landesweite-software-stoerung-citrix-problem-die-ursache/>]

28.09.2026 BSI-Warnung mit der höchsten Stufe 3 („sehr hoch“) – **bestätigt**

[<https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-289305-1032.html>]

bis 29.09.2026 watchTowr veröffentlicht Root-Cause-Analyse und PoC, danach

Massenausnutzung – **berichtet** [<https://www.helpnetsecurity.com/2026/09/29/netscaler-zero-day-exploitation-escalates-into-mass-attacks-cve-2026-88771/>]

29./30.09.2026 Rheinland-Pfalz: Ende der Störung, erste Städte melden Normalbetrieb –

berichtet [https://www.rheinpfalz.de/rheinland-pfalz_artikel,-it-sicherheitsl%C3%BCke-erste-st%C3%A4dte-melden-ende-der-st%C3%B6rung-_arid,5933974.html]

30.09.2026 Mandiant/GTIG-Erkenntnisse zu staatsnahen Akteuren, WHIPSHOT und SLAPSHOT werden öffentlich – **berichtet**

[<https://www.helpnetsecurity.com/2026/09/30/cve-2026-88772-netscaler-exploitation-zero-day/>]

01.10.2026 BSI aktualisiert die Warnung (Version 1.1); LevelBlue berichtet über privilegierte Konten und ausgeleitete Konfigurationsarchive – **bestätigt**

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

02.10.2026 CISA aktualisiert den Alert – **bestätigt** [<https://www.cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netscaler-adc-gateway>]

Vergleichsfälle

- Citrix Bleed (2023): Gestohlene Sessions und Zugangsdaten wurden noch lange nach dem Patch genutzt, später auch für Ransomware (LockBit).
- CitrixBleed 2 (2025): Edge-Geräte werden immer wieder zum Einfallstor, solange sie offen am Internet hängen und kaum überwacht werden.
- CVE-2026-3055 (NetScaler) (2026): Schon im März gab es eine aktiv ausgenutzte NetScaler-Lücke; das jetzige Advisory ist die zweite Welle in diesem Jahr.

[<https://borncity.com/blog/2026/03/30/schwachstelle-cve-2026-3055-in-citrix-netscaler-adc-und-gateway-wird-angegriffen/>]

Begriffe einfach erklärt

OT: Operational Technology – die Technik, die Anlagen wie Kraftwerke, Pumpen oder Netze steuert.

Zero-Day: Eine Lücke, die Angreifer ausnutzen, bevor der Hersteller davon weiß oder einen Patch hat.

Gateway / Remote Access: Das Eingangstor, über das Mitarbeiter und Dienstleister von außen ins Firmennetz kommen, etwa für die Fernwartung.

Edge-Geräte: Geräte am Rand des Netzes, die direkt am Internet hängen, zum Beispiel Firewalls und VPN-Gateways.

Remote Code Execution: Ein Angreifer kann aus der Ferne eigene Befehle auf dem Gerät ausführen.

Webshell: Ein kleines Schadprogramm auf einem Server, über das Angreifer jederzeit wiederkommen können.

Proof of Concept: Ein öffentlich gemachter Beispielcode, der zeigt, dass und wie eine Lücke ausnutzbar ist.

Lateral Movement: Angreifer bewegen sich vom ersten befallenen Gerät weiter ins Netz.

KEV-Katalog: Die Liste der US-Behörde CISA mit Schwachstellen, die nachweislich aktiv ausgenutzt werden.

Früherer Stand: Erstmeldung (02.10.2026 22:49)

Wissen 25 % · wahrscheinlich 15 % · nicht bekannt 60 %

Citrix hat am 27.09.2026 im Advisory CTX697096 acht Schwachstellen in NetScaler ADC und Gateway veröffentlicht. Zwei davon (CVSS v4.0 9.5) erlauben Remote Code Execution ohne Anmeldung und wurden schon Wochen vorher als Zero-Day ausgenutzt (widersprüchlich: A ab 03./04.09. / B ab 04.09. laut Unit 42 bzw. ab 05.09. laut eSentire/BSI). CISA, BSI, CERT-EU und NCSC-NL warnen, in Deutschland haben kommunale IT-Dienstleister vorsorglich abgeschaltet, eine Kompromittierung von Stadtwerken oder Versorgern in DACH ist öffentlich aber nicht belegt.

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