

VORFALL - LAGEBILD

Citrix NetScaler ADC/Gateway: neuer SAML-Zero-Day seit 02.10.2026 aktiv ausgenutzt - trifft auch gegen CVE-2026-88771/-8

Stand 03.10.2026 16:37 · Sendung: - · Belegstärke: **bestätigt** · berichtet · **vermutet** · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

Wissensstand

■ Wissen 50 % ■ Wahrscheinlich 19 % ■ Nicht bekannt 31 %

Zur Septemberkampagne ist viel belegt. Bei der neuen SAML-Lücke sind nur die Abstürze, die Bestätigung durch Citrix, die Nachstellung durch watchTowr und die Malware auf einem Honeypot gesichert. Ob die Codeausführung zuverlässig klappt, wie groß der Umfang ist und wer dahintersteckt, ist offen bzw. umstritten.

1. Was ist passiert, und warum?

WISSEN

- Seit dem Abend des 02.10.2026 kursiert ein Exploit für eine neue NetScaler-Lücke. Er funktioniert offenbar auch auf dem aktuellen Patchstand. Eine CVE und einen Patch gibt es noch nicht. (100 %) [<https://www.heise.de/news/NetScaler-Admins-aufgepasst-Zero-Day-verursacht-Crashes-und-Codeausführung-11474971.html>]
- Gepatchte NetScaler (14.1-73.37) starten wiederholt neu. Präparierte SAML-Anfragen bringen nsaaad zum Absturz, und der Watchdog löst dann ein Failover oder einen Neustart des Geräts aus. (100 %) [<https://securityonline.info/netscaler-saml-authentication-issue/>]
- Laut Citrix hängt das Problem von der Konfiguration ab (samlAction/samlIdPProfile auf Gateway/AAA) und ist „independent of the vulnerabilities disclosed in CTX697096“. Ein Security Bulletin mit Fixed Build ist angekündigt. (100 %) [<https://securityonline.info/netscaler-saml-authentication-issue/>]
- watchTowr Labs hat das Problem nachgestellt. Kevin Beaumont sah auf einem gepatchten Honeypot ein nachgeladenes Malware-Binary laufen. (100 %) [<https://www.heise.de/en/news/NetScaler-admins-beware-Zero-day-causes-crashes-and-code-execution-11474996.html>]
- Vorgeschichte: CVE-2026-88771/-88772 (CVSS 9.5) wurden schon vor dem Patch vom 27.09. als Zero-Days ausgenutzt. CISA hat sie in den KEV-Katalog aufgenommen. (100 %) [<https://www.securityweek.com/citrix-confirms-2-netscaler-zero-days-after-admins-pulled-the-plug/>]
- Mandiant/GTIG zufolge wurde CVE-2026-88772 mindestens ab Anfang September ausgenutzt, mit der Webshell WHIPSHOT und dem Tunneler SLAPSHOT. Zugeschrieben wird das einem mutmaßlich staatsnahen Akteur. (100 %) [<https://cloud.google.com/blog/topics/threat-intelligence/defending-against-active-exploitation-of-citrix-netscaler-adc-and-gateway-appliances>]
- Schon früher in 2026 gab es eine SAML-Heap-Overflow-Lücke (CVE-2026-8452, Fix in 14.1-72.61/13.1-63.18). Die SAML-Verarbeitung ist also ein wiederkehrender Schwachpunkt. (100 %) [<https://bishopfox.com/blog/no-crash-required-verifying-the-citrix-netscaler-saml-patch-for-cve-2026-8452>]

NICHT BEKANNT

- Ob die Codeausführung über die neue SAML-Lücke zuverlässig klappt und bei echten Organisationen schon gelungen ist. Citrix sieht keinen Bypass, mehrere Medien schreiben, das sei nicht unabhängig bestätigt.
- Wer hinter der SAML-Welle steckt
- Ursache im Code, CVE-Nummer und Datum des Patches

- Ob die ACSC die neue SAML-Ausnutzung bestätigt hat (widersprüchlich: der Auftrag nennt eine ACSC-Bestätigung / A findet nur die ACSC-Bestätigung für CVE-2026-88771/-88772)

WAHRSCHEINLICH (Einschätzung)

- Es gibt eine eigenständige, ausnutzbare Schwachstelle in der SAML/AAA-Verarbeitung und nicht bloß einen Stabilitätsfehler. (60 %) – Dafür sprechen Beaumonts Honeypot-Beobachtung, die Nachstellung durch watchTowr und dass die Lücke im selben Bereich sitzt. Citrix spricht aber nur von einem „issue“ ohne Bypass.
- Angreifer haben nach dem Patch gezielt nach einem Weg drumherum oder nach einer Nachbarlücke gesucht. (70 %) – Das ist ein übliches Muster nach großen Edge-Device-Kampagnen und öffentlichen PoCs (vgl. CitrixBleed, Ivanti 2024).
- Kriminelle und staatsnahe Gruppen nutzen die Lücke parallel aus. (50 %) – Schon nach dem PoC vom 29.09. gab es Massenausnutzung, und ein öffentlich kursierender Exploit senkt die Hürde.

2. Was ist die Auswirkung?

WISSEN

- Die Abstürze führen zu Failovern oder Neustarts der Appliance. Damit fällt der Remote Access aus (Denial of Service). (100 %) [<https://cybersecuritynews.com/citrix-netscaler-0-day-patch/>]
- In der PitScaler-Kampagne gab es Webshells (WHIPSHOT), Tunneling (SLAPSHOT), Root-Zugriff, Aufklärung im internen Netz, Diebstahl von Zugangsdaten und in einigen Fällen Lateral Movement. (100 %) [<https://cloud.google.com/blog/topics/threat-intelligence/defending-against-active-exploitation-of-citrix-netscaler-adc-and-gateway-appliances>]
- Mandiant berichtet über Lateral Movement ins interne Netz in einigen Fällen der Septemberkampagne. (100 %)
[<https://www.cybersecuritydive.com/news/citrix-netscaler-exploitation-days-before-notification/831634/>]
- Arctic Wolf zählt mindestens 78 angegriffene Organisationen in den USA, Kanada und Europa, unter anderem aus Energie, Gesundheitswesen und Kommunen. (100 %)
[<https://itbrief.co.uk/story/arctic-wolf-details-post-exploit-netscaler-attacks>]
- Die Arctic-Wolf-Zahl von mindestens 78 Organisationen bestätigt auch Cybersecurity Dive. (100 %) [<https://www.cybersecuritydive.com/news/exploitation-citrix-netscaler-what-we-know/831780/>]
- Beaumont verfolgt über 100 Opferorganisationen mit jeweils eigener Webshell. (100 %) [<https://www.helpnetsecurity.com/2026/09/29/netscaler-zero-day-exploitation-escalates-into-mass-attacks-cve-2026-88771/>]
- Auch SecurityWeek berichtet über die mehr als 100 Opferorganisationen. (100 %)
[<https://www.securityweek.com/government-finance-orgs-targeted-in-weeks-long-netscaler-zero-day-attacks/>]
- In den Niederlanden haben Krankenhäuser (Amphia, ETZ, Frisius MC) ihre Patientenportale vorsorglich abgeschaltet. Auf Regierungsseite wurden Citrix-Umgebungen vom Netz genommen (widersprüchlich: A nennt das Innenministerium / B sagt, die Regierung habe alle Citrix-Umgebungen vom Internet getrennt). (100 %)
[<https://www.sdxcentral.com/news/netscaler-bugs-bring-critical-sectors-down-in-europe/>]
- Das ICT Magazine berichtet ebenfalls über die abgeschalteten Portale der niederländischen Krankenhäuser und die Reaktion der Regierung. (100 %)
[<https://www.ictmagazine.nl/nieuws/nieuw-citrix-lek-treft-nederlandse-ziekenhuizen-en-overheid/>]

NICHT BEKANNT

- Welchen Schaden die neue SAML-Lücke anrichtet und ob schon Daten abgeflossen sind
- Ob gestohlene VPN-Zugangsdaten schon weiterverwendet wurden
- Ob Organisationen und Versorger in DACH betroffen sind
- Ob über NetScaler schon OT-Netze erreicht wurden. Dafür gibt es keinen öffentlichen Beleg.

WAHRSCHEINLICH (Einschätzung)

- Einige Betreiber schalten ihren Fernzugang vorsorglich ab oder schränken ihn ein, so wie in den Niederlanden. Das trifft auch die Fernwartung durch Dienstleister. (65 %) – Ohne Patch und ohne Workaround bleibt oft nur Abschalten oder Einschränken.

- Zugänge aus der Massenausnutzung werden über Initial Access Broker weiterverkauft, etwa an Ransomware-Gruppen. (60 %) – Beobachtet wurden Webshells für Botnetze und Access Brokering. Dazu kommt das Muster aus CitrixBleed 2023.

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

WISSEN

- Der Patch entfernt keine bereits gesetzten Webshells oder Backdoors. (100 %) [https://pitscaler.com/]
 - Empfohlen wird, vor dem Update forensische Snapshots anzulegen. „No Compromise Detected“ ist nicht beweiskräftig. (100 %) [https://www.bechtle.com/ueber-bechtle/newsroom/citrix-netscaler-zero-days]
 - Mandiant empfiehlt nach einer Kompromittierung, Appliance- und Admin-Zugangsdaten, SSH-Keys, TLS-Zertifikate und LDAP/RADIUS-Secrets zu rotieren, Sessions zu widerrufen 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]
 - Die ACSC rät, Systeme mindestens ab dem 04.09.2026 auf Kompromittierung zu prüfen. (100 %) [https://australiancybersecuritymagazine.com.au/acsc-warns-of-confirmed-exploitation-of-citrix-netscaler-vulnerabilities/]
 - Für die neue SAML-Lücke gibt es noch keinen Fixed Build und keinen Zeitplan. (100 %) [https://cybersecuritynews.com/citrix-netscaler-0-day-patch/]

NICHT BEKANNT

- Wann Citrix den SAML-Patch liefert
- Ob Citrix einen Workaround nachliefert
- Wie viele Geräte bereits kompromittiert sind

WAHRSCHEINLICH (Einschätzung)

- Ohne Kompromittierung dauert es Stunden bis Tage (Patch einspielen, Logs prüfen). Bei echter Kompromittierung mit Lateral Movement dauern Incident Response, Neuaufbau, Rotation der Zugangsdaten und Threat Hunting Wochen bis Monate. (70 %) – Erfahrung aus CitrixBleed 2023/2025, Ivanti 2024 und früheren NetScaler-Kampagnen.

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

WISSEN

- Betroffen sind IT-Edge-Geräte für Remote Access. Berichte über physische Schäden oder Eingriffe in die Leittechnik liegen nicht vor. Mandiant beschreibt Spionage (Webshells, Aufklärung, Diebstahl von Zugangsdaten, Tunneling) und keine Sabotage. (100 %) [https://cloud.google.com/blog/topics/threat-intelligence/defending-against-active-exploitation-of-citrix-netscaler-adc-and-gateway-appliances]

NICHT BEKANNT

- Ob bei den Energie-Opfern (Arctic Wolf) oder anderswo OT-Netze erreicht wurden
- Wie die Gateways von Versorgern an die OT angebunden sind
- Ob abgegriffene VPN-Zugangsdaten später für Zugriffe auf die Leittechnik genutzt werden

WAHRSCHEINLICH (Einschätzung)

- Diese Kampagne verursacht keinen physischen Anlagenschaden. (80 %) – Das Motiv ist Spionage bzw. der Weiterverkauf von Zugängen. Es gibt keine Berichte über Auswirkungen auf die OT.
- In Einzelfällen dient ein NetScaler als Fernwartungszugang mit Weg in die OT. Das Risiko liegt dann im späteren Lateral Movement. (40 %) – NetScaler wird auch bei Versorgern und Maschinenbauern für Remote Access genutzt, für Stadtwerke ist das aber nur allgemein belegt.
- Mittelfristig werden Zugangsdaten aus dem Fernzugang über Initial Access Broker weiterverkauft. (40 %) – Das ist ein Muster aus früheren Edge-Device-Kampagnen. Ein OT-Bezug entsteht dort, wo Dienstleister über das Gateway Fernwartung machen.

5. Wie viele solcher Ziele gibt es?

WISSEN

- Censys zählt (Stand 28.09.) 42.735 erreichbare NetScaler-Hosts weltweit. Davon stehen 5.678 in Deutschland (13 %, Platz 2 nach den USA mit 32 %), die Schweiz liegt bei rund 4 %. (100 %) [<https://censys.com/advisory/cve-2026-10747-2/>]
- Palo Alto Unit 42 sieht rund 50.000 (50.277) potenziell exponierte Instanzen. (100 %) [<https://unit42.paloaltonetworks.com/netscaler-zero-days-exploited/>]
- Securityonline nennt die Unit-42-Zahl ebenfalls. (100 %) [<https://securityonline.info/netscaler-saml-authentication-issue/>]
- Von der neuen SAML-Lücke ist nur betroffen, wer SAML auf Gateway/AAA konfiguriert hat (SAML Action bzw. SAML-IdP-Profil). (100 %) [<https://securityonline.info/netscaler-saml-authentication-issue/>]
- 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 dieser Geräte SAML nutzen
- Wie viele Versorger und KRITIS-Betreiber in DACH NetScaler als Fernzugang einsetzen
- Wie hoch die Patch-Quote in Deutschland ist

WAHRSCHEINLICH (Einschätzung)

- Ein relevanter Teil der deutschen Geräte nutzt SAML, weil viele Unternehmen das Single Sign-on mit Entra ID/Azure AD koppeln. (55 %) – SAML-SSO ist in Microsoft-365-Umgebungen ein verbreitetes Standardszenario, Zahlen dazu gibt es aber nicht.

6. Kann das wieder passieren?

WISSEN

- Laut heise ist das die dritte große NetScaler-Lücke binnen weniger Wochen. (100 %) [<https://www.heise.de/news/NetScaler-Admins-aufgepasst-Zero-Day-verursacht-Crashes-und-Codeausfuehrung-11474971.html>]
- 2026 ist das bereits die dritte kritische NetScaler-Warnung für DACH. (100 %) [https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-289305-1032.pdf?__blob=publicationFile&v=4]
- Nach dem watchTowr-PoC vom 29.09. begannen die Ausnutzungsversuche binnen Minuten (widersprüchlich bei der Quelle der Beobachtung: A nennt Lupovis / B nennt GreyNoise). (100 %) [<https://www.helpnetsecurity.com/2026/09/29/netscaler-zero-day-exploitation-escalates-into-mass-attacks-cve-2026-88771/>]

NICHT BEKANNT

- Ob weitere Lücken oder Bypässe im selben Code stecken

WAHRSCHEINLICH (Einschätzung)

- Es werden weitere kritische Lücken in Edge-Geräten als Zero-Day ausgenutzt, auch bei NetScaler (sowie Ivanti, Fortinet, Palo Alto). (85 %) – Seit CitrixBleed 2023 ist das ein wiederkehrendes Muster. Edge Devices sind der bevorzugte Initial Access staatlicher Akteure.

Lage

Seit dem Abend des 02.10.2026 bringen präparierte SAML-Anfragen den AAA-Dienst nsaaad auf Citrix NetScaler ADC/Gateway zum Absturz. Das trifft auch Geräte, die gegen die im September ausgenutzten PitScaler-Lücken CVE-2026-88771/-88772 bereits gepatcht sind (Build 14.1-73.37). Citrix bestätigt ein eigenständiges, configurationsabhängiges Problem und sieht keinen Patch-Bypass. Kevin Beaumont meldet Malware auf einem gepatchten Honeypot, watchTowr hat das Problem nachgestellt. Eine CVE, einen Patch und einen offiziellen Workaround gibt es noch nicht. In DACH ist kein Opfer namentlich bekannt, Deutschland liegt aber mit rund 5.700 erreichbaren Geräten weltweit auf Platz 2.

Angriff

Präparierte SAML-Anfragen gegen NetScaler Gateway/AAA bringen nsaaad zum Absturz, mutmaßlich auch mit Codeausführung, und zwar auch auf Geräten mit PitScaler-Patch. Vorlauf ist die PitScaler-Kampagne (CVE-2026-88771/-88772) mit der Webshell WHIPSHOT und dem Tunneler SLAPSHOT.

Wann / Status	Die SAML-Welle läuft seit dem Abend des 02.10.2026. PitScaler wird laut Mandiant seit Anfang September ausgenutzt (ab ca. 04.09.), erste Hinweise bzw. Fingerprinting gab es ab dem 21.08. (Unit 42). · laufend
Täter	Für die SAML-Welle unbekannt. Die Anfangsphase von PitScaler ordnet Mandiant (CTO Carmakal) mutmaßlich staatsnahen bzw. staatlich gesteuerten Akteuren mit Spionageziel zu, ohne eine Gruppe zu benennen. Nach dem PoC kamen opportunistische Akteure dazu (widersprüchlich bei der Belegstärke: A „unbekannt“ / B „vermutet“; für die neue Lücke gilt „unbekannt“). – unbekannt
Betreiber / Branche	· Branchenübergreifend: Behörden/Verwaltung, Finanzen, Gesundheit, Energie, Kommunen, Bildung
Anlage / Alter	IT-Edge-Gerät (Remote-Access-/VPN-Gateway, Load Balancer) · aktuell (betrifft auch Build 14.1-73.37 vom 27.09.2026)
Region	Weltweit, Schwerpunkt Nordamerika und Europa. In DE 5.678 erreichbare Geräte, kein namentliches DACH-Opfer bekannt.

Angriffsvektor

Bekannt: Unauthentifizierte, präparierte SAML-Anfragen an aus dem Internet erreichbare Gateway/AAA-vServer. Betroffen sind nur Geräte mit SAML-Konfiguration (Citrix via securityonline, heise, cybersecuritynews). Technische Details sind bewusst weggelassen.

- Eigenständige Speicherfehler-Schwachstelle in der SAML-Verarbeitung von nsaaad (neue Lücke, kein Bypass) (hoch): Citrix nennt ein eigenständiges Problem, und das SAML-Parsing war 2026 schon einmal betroffen (CVE-2026-8452). Eine Alternative halten wir für gering wahrscheinlich: Die Malware stammt von Persistenz, die vor dem Patch eingerichtet wurde, und wird fälschlich der neuen Lücke zugeschrieben. Dagegen spricht, dass Honeypots in der Regel frisch aufgesetzt sind.
- Unvollständiger Fix der PitScaler- oder der CVE-2026-8452-Fehlerklasse (mittel): Beaumont spricht von „PitScaler 2“, Citrix bestreitet einen Bypass.
- Initial Access über das Gateway, danach Abgriff von VPN-Zugangsdaten, Lateral Movement in Richtung Fernwartungszugänge von Versorgern oder Weiterverkauf über Initial Access Broker an Ransomware-Gruppen (mittel): Das Muster ist aus der Septemberkampagne belegt (Superuser-Konten, Zugangsdaten) und typisch nach massenhaft ausgenutzten Edge-Lücken (CitrixBleed 2023). Bei Versorgern führt der Weg zur OT häufig über die Fernwartung.
- Ungezielte Störung durch massenhafte Abstürze (DoS) des Fernzugangs (hoch): Die Abstürze sind breit gemeldet, und ein öffentlicher Exploit wird erfahrungsgemäß auch ungezielt eingesetzt.

Zeitleiste

30.06.–18.08.2026 SAML-Heap-Overflow CVE-2026-8452 gepatcht (CTX696604), watchTowr-Analyse am 14.08. – [berichtet](#)

[<https://arcticwolf.com/resources/blog/citrix-netscaler-adc-gateway-critical-rce-vulnerability-cve-2026-8452/>]

21.08.2026 Erstes Fingerprinting von NetScaler-Geräten und erste Hinweise auf PitScaler-Aktivität – [berichtet](#) [<https://unit42.paloaltonetworks.com/netscaler-zero-days-exploited/>]

Anfang 09.2026 (ab ca. 04.09.) Zero-Day-Ausnutzung von CVE-2026-88772, Webshells WHIPSHOT und Tunneler SLAPSHOT – [bestätigt](#) [<https://cloud.google.com/blog/topics/threat-intelligence/defending-against-active-exploitation-of-citrix-netscaler-adc-and-gateway-appliances>]

25.09.2026 Die niederländische Regierung erhält eine vertrauliche Warnung eines europäischen Partners – [berichtet](#) [<https://pitscaler.com/>]

27.09.2026 Citrix veröffentlicht Patches (CTX697096), CISA nimmt CVE-2026-88771/-88772 in den KEV-Katalog auf – [bestätigt](#)

[<https://www.securityweek.com/citrix-confirms-2-netcaler-zero-days-after-admins-pulled-the-plug/>]

28.09.2026 Behörden warnen (u. a. ACSC: Ausnutzung bestätigt, Prüfung ab 04.09.).
Niederländische Krankenhäuser schalten ihre Patientenportale ab. Censys zählt 5.678
erreichbare Geräte in Deutschland. – [berichtet](#)

[<https://www.dutchnews.nl/2026/09/hospitals-block-access-to-patients-records-after-cyber-threat/>]

29.09.2026 watchTowr veröffentlicht einen PoC, binnen Minuten beginnt die Massenausnutzung.
Beaumont zählt über 100 Opferorganisationen mit Webshells. – [berichtet](#) [<https://www.helpnetsecurity.com/2026/09/29/netcaler-zero-day-exploitation-escalates-into-mass-attacks-cve-2026-88771/>]

02.10.2026 (abends) Neuer SAML-Exploit: nsaaad stürzt auch auf gepatchten Geräten ab,
Malware auf einem gepatchten Honeypot, watchTowr stellt das Problem nach. Citrix bestätigt ein
eigenständiges Problem, es gibt keine CVE und keinen Patch. – [berichtet](#) [<https://www.heise.de/news/Netcaler-Admins-aufgepasst-Zero-Day-verursacht-Crashes-und-Codeausfuehrung-11474971.html>]

02./03.10.2026 Citrix-Stellungnahme: Das Problem hängt von der Konfiguration ab (SAML auf
Gateway/AAA) und ist unabhängig von CTX697096. Bulletin und Fixed Build sind angekündigt. –
[bestätigt](#) [<https://securityonline.info/netcaler-saml-authentication-issue/>]

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