



NCSC-2026-0216

Kwetsbaarheden verholpen in Citrix Netscaler ADC en Netscaler Gateway

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 18-08-2026

Revisie: 1.0.1

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 1

Inmiddels hebben onderzoekers ook Code Executie weten te bereiken.

Feiten

Citrix heeft kwetsbaarheden verholpen in NetScaler ADC en NetScaler Gateway die verband houden met onvoldoende invoervalidatie, onjuiste toegangscontrole en het onjuist vrijgeven van geheugen.

Duiding

De kwetsbaarheden met de kenmerken CVE-2026-8451 en CVE-2026-10817 ontstaan door onvoldoende invoervalidatie, waarbij de software invoergroottes en -grenzen niet correct controleert. Dit kan leiden tot geheugenoverlezingen, wat kan resulteren in ongeautoriseerde openbaarmaking van gevoelige informatie, wanneer de producten zijn geconfigureerd als SAML IDP, of als TCP TimeStamp is ingeschakeld bij een TCP-profiel dat is gekoppeld aan een virtuele server van het type: Load Balancing (LB), Content Switching (CS) of VPN.

De kwetsbaarheden met de kenmerken CVE-2026-8452 en CVE-2026-8655 bevinden zich in de manier waarop geheugen wordt beheerd in NetScaler ADC en NetScaler Gateway. Dit kan leiden tot een denial-of-service (DoS) of een ongewenste control flow wanneer de producten zijn geconfigureerd als Gateway, DNS-proxy, recursieve DNS-resolver of AAA-virtuele server.

De kwetsbaarheid met het kenmerk CVE-2026-13474 ontstaat door het onjuist vrijgeven van geheugen. Kwaadwillenden kunnen deze kwetsbaarheid misbruiken door via speciaal geprepareerde HTTP/2-verzoeken een denial-of-service (DoS) te veroorzaken.

De kwetsbaarheid met het kenmerk CVE-2026-10816 betreft een probleem met de toegangscontrole binnen de Management Interface. Niet-geauthenticeerde kwaadwillenden op afstand kunnen de kwetsbaarheid misbruiken om willekeurige bestanden uit te lezen. Dit kan resulteren in ongeautoriseerde openbaarmaking van gevoelige informatie.

Onderzoekers hebben Proof-of-Concept (PoC) code gedeeld waarmee de kwetsbaarheid met kenmerk CVE-2026-8451 kan worden aangetoond.

UPDATE: Inmiddels hebben dezelfde onderzoekers ook Proof-of-Concept (PoC) code gepubliceerd waarmee uitvoer van willekeurige code mogelijk wordt. Het kwetsbare systeem moet hiervoor wel zijn geconfigureerd om middels SAML ingezet te zijn als Identity Provider. Dit is geen gebruikelijke configuratie, omdat best practices adviseren het Identity Management en Access Management gescheiden te houden.

Oplossingen

Citrix heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Het NCSC adviseert organisaties om de door Citrix beschikbaar gestelde beveiligingsupdate op korte termijn te installeren. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-8451	8.8 HIGH
➤ CVE-2026-8452	8.8 HIGH
➤ CVE-2026-8655	8.8 HIGH
➤ CVE-2026-10816	7.1 HIGH
➤ CVE-2026-10817	6.9 MEDIUM
➤ CVE-2026-13474	8.7 HIGH

CWE's

CWE	Beschrijving
➤ CWE-73	External Control of File Name or Path
➤ CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
➤ CWE-125	Out-of-bounds Read
➤ CWE-401	Missing Release of Memory after Effective Lifetime

Getroffen producten

NetScaler
ADC
Gateway

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.