



NCSC-2026-0100

Kwetsbaarheden verholpen in Citrix Netscaler ADC en Netscaler Gateway

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 23-03-2026

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

Feiten

Citrix heeft kwetsbaarheden verholpen in hun software die verband houden met onvoldoende invoervalidatie en een raceconditie in het sessiebeheer.

Duiding

De kwetsbaarheid in de invoervalidatie ontstaat doordat de software niet correct controleert op invoergroottes of -grenzen, wat kan leiden tot geheugenoverlezingen. Dit kan resulteren in ongeautoriseerde openbaarmaking van gevoelige informatie of destabilisatie van de applicatie. De raceconditie in het sessiebeheer leidt tot onjuiste behandeling van gebruikerssessies, wat kan resulteren in sessiemix-ups en compromittering van de integriteit en vertrouwelijkheid van gebruikerssessies. Dit kan gevoelige informatie blootstellen of ongeautoriseerde toegang mogelijk maken.

Oplossingen

Citrix heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300&articleURL=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2026_3055_and_CVE_2026_4368

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-3055	9.3 CRITICAL
➤ CVE-2026-4368	7.7 HIGH

CWE's

CWE	Beschrijving
➤ CWE-125	Out-of-bounds Read
➤ CWE-362	

Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Getroffen producten

Citrix

NetScaler
ADC

NetScaler
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.