



NCSC-2025-0268

Kwetsbaarheden verholpen in Citrix NetScaler ADC en Gateway

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 26-08-2025

Revisie: 1.0.2

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 2

Nader onderzoek toont aan dat de kwetsbare configuratie zeer veel voorkomt waardoor grootschalig misbruik waarschijnlijk wordt.

Feiten

Citrix heeft kwetsbaarheden verholpen in de NetScaler ADC en Gateway

Duiding

De kwetsbaarheden zijn gerelateerd aan geheugenoverflow en onjuiste toegangscontroleconfiguraties. Kwaadwillenden kunnen de kwetsbaarheden misbruiken om een Denial-of-Service te veroorzaken en mogelijk willekeurige code uit te voeren op het kwetsbare systeem. De kwetsbaarheden zijn van toepassing op de On-Premise installaties van ADC en Gateway. De cloudoplossingen zijn door Citrix inmiddels gepatched.

Citrix meldt berichten te hebben ontvangen dat de kwetsbaarheid met kenmerk CVE-2025-7775 actief is misbruikt.

De kwetsbare configuratie die door Citrix is aangegeven is dermate veel voorkomend dat het NCSC op korte termijn grootschalig misbruik verwacht. Het NCSC adviseert met klem de update zo spoedig mogelijk te installeren.

Oplossingen

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

Het NCSC heeft eerder een detectiescript gepubliceerd waarmee compromittatie kan worden gedetecteerd. Dit script is ontwikkeld om compromittatie te detecteren voor de kwetsbaarheid met kenmerk CVE-2025-6543. Dit script is ook geschikt om compromittatie door middel van latere kwetsbaarheden te detecteren. Het NCSC raadt aan om dit script uit te voeren op NetScaler systemen.

Voor de oudere kwetsbaarheden heeft het NCSC beveiligingsadviezen [NCSC-2025-0203](#) en [NCSC-2025-0196](#) gepubliceerd.

Het detectiescript kan worden verkregen via https://github.com/NCSC-NL/citrix-2025/blob/main/live-host-bash-check/TLPCLEAR_check_script_cve-2025-6543-v1.8.sh

De handleiding voor dit script kan worden verkregen via <https://github.com/NCSC-NL/citrix-2025/blob/main/live-host-bash-check/README.md>

Referenties

- <https://advisories.ncsc.nl/2025/ncsc-2025-0196.html>
- <https://advisories.ncsc.nl/2025/ncsc-2025-0203.html>
- <https://github.com/NCSC-NL/citrix-2025/blob/main/live-host-bash-check/README.md>
- https://github.com/NCSC-NL/citrix-2025/blob/main/live-host-bash-check/TLPCLEAR_check_script_cve-2025-6543-v1.8.sh
- https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694938&articleTitle=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2025_7775_CVE_2025_7776

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-7775	9.2 CRITICAL
➤ CVE-2025-7776	8.8 HIGH
➤ CVE-2025-8424	8.7 HIGH

CWE's

CWE	Beschrijving
➤ CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
➤ CWE-284	Improper Access Control

Getroffen producten

Citrix
NetScaler ADC 12.1-FIPS
NetScaler ADC 12.1-NDcPP
NetScaler ADC 13.1-FIPS
NetScaler ADC 13.1-NDcPP
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.