



NCSC-2025-0196

Kwetsbaarheden verholpen in Citrix NetScaler ADC en NetScaler Gateway

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 08-07-2025

Revisie: 1.0.3

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 3

Het NCSC acht het waarschijnlijk dat deze kwetsbaarheden op korte termijn zullen worden misbruikt. De inschaling is daarom aangepast naar H/H. Het NCSC adviseert organisaties met klem om de door Citrix beschikbaar gestelde beveiligingsupdates op korte termijn te installeren.

Feiten

Citrix heeft kwetsbaarheden verholpen in NetScaler ADC en NetScaler Gateway.

Duiding

De kwetsbaarheid met kenmerk CVE-2025-5777 betreft een Out-of-Bounds Read. Deze kwetsbaarheid ontstaat door onvoldoende invoervalidatie in systemen die zijn geconfigureerd als Gateway-diensten. Dit betreft onder andere VPN-virtual servers, ICA Proxy, Citrix Virtual Private Network (CVPN), Remote Desktop Protocol (RDP) Proxy en AAA-servers. In tegenstelling tot eerdere informatie van Citrix bevindt deze kwetsbaarheid zich **niet** in de management-interface. Deze kwetsbaarheid is daarmee op afstand te misbruiken door een kwaadwillende zonder voorafgaande authenticatie.

Voor deze kwetsbaarheid is Proof-of-Concept-code (PoC) verschenen. De kans op een toename in scanverkeer en pogingen tot misbruik wordt hierdoor significant groter.

De tweede kwetsbaarheid met kenmerk CVE-2025-5349, betreft een probleem met onjuiste toegangscontrole binnen de NetScaler Management Interface. Kwaadwillenden kunnen de kwetsbaarheid misbruiken voor het verkrijgen van ongeautoriseerde toegang tot bepaalde onderdelen van het systeem. Hiervoor heeft de kwaadwillende toegang nodig tot specifieke netwerkinterfaces, zoals het Network Services IP (NSIP), het Cluster Management IP of het lokale Global Server Load Balancing (GSLB) Site IP.

Oplossingen

Citrix heeft updates uitgebracht om deze kwetsbaarheden te verhelpen.

Citrix raadt aan om alle actieve ICA- en PCoIP-sessies te beëindigen nadat de beveiligingsupdates zijn geïnstalleerd. Raadpleeg het beveiligingsadvies van Citrix voor aanvullende informatie.

Updates beschikbaar voor de volgende NetScaler-versies:

- NetScaler ADC en NetScaler Gateway vanaf versie 14.1-43.56
- NetScaler ADC en NetScaler Gateway 13.1 vanaf versie 13.1-58.32
- NetScaler ADC 13.1-FIPS en 13.1-NDcPP vanaf versie 13.1-37.235
- NetScaler ADC 12.1-FIPS vanaf versie 12.1-55.328

Het NCSC adviseert organisaties met klem om de door Citrix beschikbaar gestelde beveiligingsupdates op korte termijn te installeren.

Referenties

- <https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420>
- <https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694729>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-5777	9.3 CRITICAL
➤ CVE-2025-5349	8.7 HIGH

CWE's

CWE	Beschrijving
➤ CWE-1284	Improper Validation of Specified Quantity in Input
➤ CWE-284	Improper Access Control

Getroffen producten

Citrix
Netscaler ADC, NetScaler Gateway
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 or 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.