Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0318

Kwetsbaarheden verholpen in Citrix NetScaler ADC en NetScaler Gateway

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 07-09-2026
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

Publieke PoC code beschikbaar waardoor actiefmisbruik op korte termijn te verwachten is.

Feiten

Citrix heeft kwetsbaarheden verholpen in NetScaler ADC en NetScaler Gateway.

Duiding

De kwetsbaarheid met kenmerk CVE-2026-19489 betreft een memory overflow in NetScaler ADC en NetScaler Gateway, wanneer de producten zijn geconfigureerd als SIP ALG binnen een Large Scale NAT (LSN) groep. Deze fout in de geheugenallocatie kan leiden tot onvoorspelbaar gedrag of een denial of service, waardoor de normale werking van het systeem verstoord kan worden.

De kwetsbaarheid met kenmerk CVE-2026-19490 maakt het voor een aanvaller mogelijk om via een alternatieve route de normale authenticatiemechanismen te omzeilen, om zodoende ongeautoriseerde toegang tot het systeem te verkrijgen. Om kwetsbaar te zijn moeten de producten in combinatie met specifieke versies geconfigureerd zijn als Gateway (VPN-virtuele server, ICA Proxy, CVPN, RDP Proxy), AAA virtual server of configureerd zijn als SAML Identity Provider. Dit laatste is geen gebruikelijke configuratie.

UPDATE

Er is Proof of Concept code beschikbaar voor CVE-2026-19490. Het NCSC acht het zeer waarschijnlijk dat op korte termijn misbruik zal plaatsvinden.

Oplossingen

Citrix heeft updates uitgebracht om deze kwetsbaarheden in NetScaler ADC en NetScaler Gateway te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696939

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-19489	8.8 HIGH

CVE-2026-19490	**9.3 CRITICAL**

CWE's

CWE	Beschrijving
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-288	Authentication Bypass Using an Alternate Path or Channel

Getroffen producten

Citrix
NetScaler ADC and NetScaler Gateway
NetScaler
ADC
Gateway

Disclaimer