Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0216

Kwetsbaarheden verholpen in Citrix Netscaler ADC en Netscaler Gateway

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 30-06-2026

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 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.

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