Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0394

Kwetsbaarheden verholpen in NetScaler ADC en NetScaler Gateway

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 27-09-2026

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 8 kwetsbaarheden verholpen in NetScaler ADC en NetScaler Gateway. De volgende ondersteunde versies van Citrix NetScaler ADC en Citrix NetScaler Gateway zijn kwetsbaar:

- Citrix NetScaler ADC en Citrix NetScaler Gateway 14.1 vóór versie 14.1-73.37
- Citrix NetScaler ADC en Citrix NetScaler Gateway 13.1 vóór versie 13.1-64.23
- Citrix NetScaler ADC FIPS vóór versie 14.1-73.37 FIPS
- Citrix NetScaler ADC FIPS en NDcPP vóór versie 13.1-37.279

Secure Private Access Hybrid-implementaties die gebruikmaken van NetScaler-instances zijn ook kwetsbaar voor deze kwetsbaarheden.

Deze advisory is uitsluitend van toepassing op door klanten beheerde Citrix NetScaler ADC-systemen (“NetScaler ADC”) en Citrix NetScaler Gateway-systemen (“NetScaler Gateway”). Cloud Software Group voorziet de door Citrix beheerde clouddiensten en Citrix Managed Adaptive Authentication van de benodigde software-updates.

Duiding

De kwetsbaarheden betreffen verschillende beveiligingsproblemen die onder meer kunnen leiden tot Remote Code Execution (RCE), HTTP Request Smuggling, het omzeilen van beleidsregels en Denial-of-Service. Drie kwetsbaarheden met kenmerk CVE-2026-88771, CVE-2026-88772 en CVE-2026-88773 zijn als kritiek aangemerkt.

De kwetsbaarheid met kenmerk CVE-2026-88771 heeft een CVSS-score van 9,5 en betreft onvoldoende invoervalidatie. Een niet-geauthenticeerde kwaadwillende kan op afstand willekeurige commando's uitvoeren. Volgens Citrix zijn alle NetScaler ADC- en NetScaler Gateway-deployments getroffen en is geen aanvullende functionaliteit of specifieke configuratie voor misbruik vereist.

De kwetsbaarheid met kenmerk CVE-2026-88772 heeft een CVSS-score van 9,5 en betreft een memory overflow die kan leiden tot RCE of Denial-of-Service. Misbruik is mogelijk wanneer DTLS is ingeschakeld. Citrix geeft aan dat DTLS standaard is ingeschakeld op een VPN virtual server.

De kwetsbaarheid met kenmerk CVE-2026-88773 heeft een CVSS-score van 9,3 en betreft HTTP Request Smuggling. Voor misbruik moet HTTP-functionaliteit zijn ingeschakeld op NetScaler ADC of NetScaler Gateway. Authenticatie en gebruikersinteractie zijn niet vereist.

De kwetsbaarheid met kenmerk CVE-2026-88774 heeft een CVSS-score van 7,0 en kan leiden tot het omzeilen van een feature policy door onjuist gebruik van HTTP URL-gebaseerde policy expressions. De kwetsbaarheid is alleen van toepassing wanneer dergelijke expressions zijn geconfigureerd.

De kwetsbaarheid met kenmerk CVE-2026-88775 heeft een CVSS-score van 8,8 en betreft een memory overflow die kan leiden tot onvoorspelbaar gedrag of Denial-of-Service. De kwetsbaarheid is van toepassing op

systemen die zijn geconfigureerd als Gateway, waaronder SSL VPN, ICA Proxy, CVPN en RDP Proxy, of als AAA virtual server.

De kwetsbaarheid met kenmerk CVE-2026-88776 heeft een CVSS-score van 8,8 en betreft eveneens een memory overflow die kan leiden tot onvoorspelbaar gedrag of Denial-of-Service. Voor misbruik moet een load-balancing virtual server van het type Oracle zijn geconfigureerd.

De kwetsbaarheid met kenmerk CVE-2026-88777 heeft een CVSS-score van 8,8 en betreft een memory overflow die kan leiden tot onvoorspelbaar gedrag of Denial-of-Service. De kwetsbaarheid vereist een LB-, CS- of CGNAT-LSN/NAT64-configuratie waarbij een non-HTTP Layer 7-protocol is ingeschakeld.

De kwetsbaarheid met kenmerk CVE-2026-88778 heeft een CVSS-score van 8,8 en betreft voorspelbaarheid van TCP Initial Sequence Numbers (ISN). Voor misbruik moet TCP-functionaliteit zijn ingeschakeld op NetScaler ADC of NetScaler Gateway.

Citrix meldt dat misbruik van de kwetsbaarheden met kenmerk CVE-2026-88771 en CVE-2026-88772 zijn waargenomen op NetScaler-systemen.

Oplossingen

Citrix heeft beveiligingsupdates uitgebracht om de kwetsbaarheden te verhelpen. Het NCSC adviseert om de beveiligingsupdates met spoed toe te passen.

Vanwege het bevestigde misbruik van de kwetsbaarheden met kenmerk CVE-2026-88771 en CVE-2026-88772 wordt geadviseerd om bij systemen die vóór het installeren van de update waren blootgesteld, ook rekening te houden met mogelijke eerdere compromittatie.

Voordat de update wordt doorgevoerd, wordt geadviseerd relevante logging en een memory dump veilig te stellen. Hierdoor blijft mogelijk forensisch bewijsmateriaal beschikbaar voor onderzoek naar eerder misbruik. Het installeren van de update voorkomt nieuwe misbruik, maar sluit niet uit dat eerder al misbruik heeft plaatsgevonden. Zie bijgevoegde referenties voor meer informatie.

Referenties

› https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096&articleTitle=Citrix_NetScaler_ADC_and_Citrix_NetScaler_Gateway_Security_Bulletin_for_CVE_2

Kwetsbaarheden

CVE	CVSS Score
› CVE-2026-88771	9.5 CRITICAL

CVE-2026-88772	9.5 CRITICAL
CVE-2026-88773	9.3 CRITICAL
CVE-2026-88774	7.0 HIGH
CVE-2026-88775	8.8 HIGH
CVE-2026-88776	8.8 HIGH
CVE-2026-88777	8.8 HIGH
CVE-2026-88778	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-342	Predictable Exact Value from Previous Values
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

Getroffen producten

Citrix
NetScaler ADC
NetScaler Gateway

Disclaimer