Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0491

PRIORITEIT: NORMAAL

Meerdere kwetsbaarheden verholpen in Citrix Secure Access Client, NetScaler ADC, NetScaler Gateway en NetScaler Console.

Publicatiedatum: 12-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Citrix heeft meerdere kwetsbaarheden verholpen in Citrix Secure Access Client, NetScaler ADC, NetScaler Gateway en NetScaler Console.

Duiding

Citrix heeft meerdere kwetsbaarheden verholpen in Citrix Secure Access Client for Windows, NetScaler ADC, NetScaler Gateway en NetScaler Console. De kwetsbaarheden hebben CVSS v4.0-scores variërend van 6.9 tot 9.5 en omvatten onder andere geheugenbeschadiging (Memory Corruption), authenticatieomzeiling (Improper Authentication) en privilege-escalatie (Improper Privilege Management).

Misbruik van de kwetsbaarheden kan leiden tot Denial-of-Service, ongeautoriseerde toegang tot afgeschermde resources of het verkrijgen van SYSTEM-rechten op een Windows-systeem. Meerdere kwetsbaarheden in NetScaler ADC en Gateway kunnen op afstand worden misbruikt zonder voorafgaande authenticatie. Voor andere kwetsbaarheden is lokale toegang of een specifieke productconfiguratie vereist.

Oplossingen

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

Referenties

- https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697280&articleTitle=Citrix_Secure_Access_Client_for_Windows_Security_Bulletin_for_CVE_2026_118268
- https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697305&articleTitle=Citrix_NetScaler_ADC_and_Citrix_NetScaler_Gateway_Security_Bulletin
- https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697320&articleTitle=Citrix_NetScaler_Console_Security_Bulletin_for_CVE_2026_120869

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-107407	9.3 CRITICAL
CVE-2026-107408	9.3 CRITICAL
CVE-2026-107409	9.3 CRITICAL
CVE-2026-107410	9.3 CRITICAL
CVE-2026-107411	8.7 HIGH
CVE-2026-107412	9.5 CRITICAL
CVE-2026-107413	8.7 HIGH
CVE-2026-107414	
CVE-2026-107415	
CVE-2026-111340	
CVE-2026-111341	
CVE-2026-111342	
CVE-2026-111343	5.3 MEDIUM
CVE-2026-111344	5.3 MEDIUM
CVE-2026-111345	5.3 MEDIUM
CVE-2026-111346	5.3 MEDIUM
CVE-2026-111347	8.2 HIGH
CVE-2026-111348	5.3 MEDIUM
CVE-2026-111349	6.9 MEDIUM
CVE-2026-118268	8.5 HIGH
CVE-2026-120860	
CVE-2026-120861	
CVE-2026-120862	
CVE-2026-120863	
CVE-2026-120864	
CVE-2026-120865	
CVE-2026-120866	
CVE-2026-120867	
CVE-2026-120868	9.3 CRITICAL

CVE	CVSS Score
CVE-2026-120869	

CWE's

CWE	Beschrijving
CWE-321	Use of Hard-coded Cryptographic Key
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-787	Out-of-bounds Write
CWE-862	Missing Authorization

Getroffen producten

Citrix
NetScaler
NetScaler ADC
NetScaler ADC and NetScaler Gateway
Secure Access Client for Windows

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.