



An Láirionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2610090281

NCSC Advisory

Critical Vulnerability in Citrix NetScaler ADC and Gateway

CVE-2026-107406

9th, October 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see <https://www.first.org/tlp/>.
Please treat this document in accordance with the TLP assigned.



Description

CVE ID: CVE-2026-107406

Published: 2026-10-08

Vendor: Citrix

Product: Netscaler Gateway, ADC

CVSS Score¹: 9.5

Products Affected

Product	Version
ADC	0 < 14.1-73.46
ADC	0 < 13.1-64.29
ADC	0 < 14.1-73.46 FIPS
ADC	0 < 13.1.37.283 FIPS
Gateway	0 < 14.1-73.46
Gateway	0 < 13.1-64.29

Impact

Memory overflow vulnerability in NetScaler ADC and NetScaler Gateway when configured as a SAML Service Provider (SP) or SAML Identity Provider (IdP) that can lead to Remote Code Execution or Denial of Service.

NetScaler ADC or NetScaler Gateway must be configured as a SAML SP or SAML IdP, subject to the following version-specific requirements:

For the following versions: Applicable only when configured as a SAML IdP:

- NetScaler ADC and NetScaler Gateway between 14.1-73.37 and 14.1-73.41, inclusive
- NetScaler ADC 14.1-FIPS between 14.1-73.37 FIPS and 14.1-73.41 FIPS, inclusive

¹ <https://www.first.org/cvss/>



- NetScaler ADC and NetScaler Gateway between 13.1-64.23 and 13.1-64.28, inclusive
- NetScaler ADC 13.1-FIPS between 13.1-NDcPP 13.1-37.279 and 13.1- 37.282, inclusive

For the following versions: Applicable only when configured as a SAML SP or SAML IdP:

- NetScaler ADC and NetScaler Gateway before 14.1-73.37
- NetScaler ADC 14.1-FIPS before 14.1-73.37 FIPS
- NetScaler ADC and NetScaler Gateway before 13.1-64.23
- NetScaler ADC 13.1-FIPS before 13.1-NDcPP 13.1-37.279

Common Weakness Enumeration (CWE)²: CWE-119 - Improper Restriction of Operations within the Bounds of a Memory Buffer

Known Exploited Vulnerability (KEV) catalog³: No

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Citrix.

- <https://nvd.nist.gov/vuln/detail/CVE-2026-107406>
- <https://www.cve.org/CVERecord?id=CVE-2026-107406>
- <https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697191>

² <https://cwe.mitre.org>

³ <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>