An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2603230224

NCSC Advisory

Vulnerabilities in Citrix NetScaler ADC and NetScaler Gateway

CVE-2026-3055, CVE-2026-4368

24th, March 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-2026-3055

Published: 2026-03-23

Vendor: Citrix

Product: NetScaler ADC and NetScaler Gateway, NetScaler ADC FIPS and NDcPP

CVSS Score[1]: 9.3

CVE ID: CVE-2026-4368

Published: 2026-03-23

Vendor: Citrix

Product: NetScaler ADC and NetScaler Gateway

CVSS Score[2]: 7.7

Products Affected

CVE-2026-3055:

Product	Version
NetScaler ADC and NetScaler Gateway	14.1 < 14.1-66.59
NetScaler ADC and NetScaler Gateway	13.1 < 13.1-62.23
NetScaler ADC FIPS and NDcPP	< 13.1-37.262

CVE-2026-4368:

Product	Version
NetScaler ADC and NetScaler Gateway	14.1-66.54

Impact

[1] https://www.first.org/cvss/
[2] https://www.first.org/cvss/

CVE-2026-3055:

Insufficient input validation leading to memory overread. The pre-conditions for this are that Citrix ADC or Citrix Gateway must be configured as a SAML IDP.

Common Weakness Enumeration (CWE)[3]: CWE-125: Out-of-bounds Read

Known Exploited Vulnerability (KEV) catalog[4]: No

Used by Ransomware Operators: N/A

CVE-2026-4368:

Race Condition leading to User Session Mixup. The pre-conditions for this are that the appliance must be configured as:

Gateway (SSL VPN, ICA Proxy, CVPN, RDP Proxy) **OR** AAA virtual server

Common Weakness Enumeration (CWE)[5]: CWE-362: Race Condition

Known Exploited Vulnerability (KEV) catalog[6]: No

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Customers are recommended to upgrade their appliances to one of the supported versions that address the vulnerabilities. Affected organisations should review the latest release notes and install the relevant updates from Citrix.

Affected customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions as soon as possible:

- NetScaler ADC and NetScaler Gateway 14.1-66.59 and later releases
- NetScaler ADC and NetScaler Gateway 13.1-62.23 and later releases of 13.1
- NetScaler ADC 13.1-FIPS and 13.1-NDcPP 13.1.37.262 and later releases of 13.1-FIPS and 13.1-NDcPP

[3] https://cwe.mitre.org
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[5] https://cwe.mitre.org
[6] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CVE-2026-3055:

Customers can determine if they have an appliance configured as a SAML IDP Profile by inspecting their NetScaler Configuration for the specified string:

- add authentication samlIdPProfile .*

CVE-2026-4368:

Customers can determine if they have an appliance configured as one of the following by inspecting their NetScaler Configuration for the specified strings:

- An Auth Server (AAA Vserver):
    - add authentication vserver .*
- A Gateway (VPN Vserver, ICA Proxy, CVPN, RDP Proxy) :
    - add vpn vserver .*

https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300&articleURL=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2026_3055_and_CVE_2026_4368