An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2609270214

NCSC Advisory

Multiple Critical Vulnerabilities in Citrix NetScaler Gateway & ADC

27th September 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

Multiple vulnerabilities have been discovered in Citrix NetScaler ADC (formerly Citrix ADC) and Citrix NetScaler Gateway (formerly Citrix Gateway).

Exploits of CVE-2026-88771 and CVE-2026-88772 on unmitigated NetScaler deployments have been observed.

NOTE: Secure Private Access Hybrid deployments using NetScaler instances are also affected by the vulnerabilities. Citrix customers need to upgrade these NetScaler instances to the recommended NetScaler builds to address the vulnerabilities.

Products Affected

The following supported versions of Citrix NetScaler ADC and Citrix NetScaler Gateway are affected by the vulnerabilities:

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

CVE Details

CVE ID: CVE-2026-88771

Published: 2026-09-27

Vendor: Citrix NetScaler

Product: Gateway, ADC

CVSS Score[1]: 9.5

Common Weakness Enumeration (CWE)[2]: CWE-20 Improper input validation

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

CVE ID: CVE-2026-88772

Published: 2026-09-27

Vendor: Citrix NetScaler

Product: ADC, Gateway

CVSS Score: 9.5

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

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CVE ID: CVE-2026-88773

Published: 2026-09-27

Vendor: Citrix NetScaler

Product: ADC, Gateway

CVSS Score: 9.3

Common Weakness Enumeration (CWE): CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

CVE ID: CVE-2026-88774

Published: 2026-09-27

Vendor: Citrix NetScaler

Product: ADC, Gateway

CVSS Score: 7.0

Common Weakness Enumeration (CWE): CWE-16: Configuration

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

CVE ID: CVE-2026-88775

Published: 2026-09-27

Vendor: Citrix NetScaler

Product: ADC, Gateway

CVSS Score: 8.0

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

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

CVE ID: CVE-2026-88776

Published: 2026-09-27

Vendor: Citrix NetScaler

Product: ADC, Gateway

CVSS Score: 8.8

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

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

CVE ID: CVE-2026-88777

Published: 2026-09-27

Vendor: Citrix NetScaler

Product: ADC, Gateway

CVSS Score: 8.8

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

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

CVE ID: CVE-2026-88778

Published: 2026-09-27

Vendor: Citrix NetScaler

Product: ADC, Gateway

CVSS Score: 8.8

Common Weakness Enumeration (CWE): CWE-342: Predictable Exact Value from Previous Values

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates with the highest priority. Affected organisations should review the latest release notes and install the relevant updates from Citrix. Patricular attention should be paid to the "**Steps to determine if an appliance meets the CVE preconditions**" section in the Citrix advisory.

NOTE: NetScaler deployments impacted by CVE-2026-88778 should apply the TCP configuration change as mentioned in https://docs.netscaler.com/en-us/citrix-adc/current-release/system/tcp-configurations.html#enhanced-isn-generation

- https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096&articleTitle=Citrix_NetScaler_ADC_and_Citrix_NetScaler_Gateway_Security_Bulletin_for_CVE_2026_88771_CVE_2026_88772_CVE_2026_88773_CVE_2026_88774_CVE_2026_88775_CVE_2026_88776_CVE_2026_88777_and_CVE_2026_88778