An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2611130282

NCSC Advisory

Multiple Critical Vulnerabilities in Citrix NetScaler Gateway & ADC

13th, November 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). Refer below for further details.

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 14.1-73.57
- Citrix NetScaler ADC and Citrix NetScaler Gateway 13.1 BEFORE 13.1-64.39
- Citrix NetScaler ADC FIPS BEFORE 14.1-73.58 FIPS
- Citrix NetScaler ADC FIPS and NDcPP BEFORE 13.1-37.293

CVE Details

CVE ID: CVE-2026-120868

Published: 2026-11-12

Vendor: Citrix NetScaler

Product: ADC, Gateway

CVSS Score[1]: 9.3

Common Weakness Enumeration (CWE)[2]: CWE-119,

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

Used by Ransomware Operators: N/A

CVE ID: CVE-2026-107407

Published: 2026-11-12

Vendor: Citrix NetScaler

Product: ADC, Gateway

CVSS Score[4]: 9.3

Common Weakness Enumeration (CWE)[5]: CWE-119

Known Exploited Vulnerability (KEV) catalog[6]: 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
[4] https://www.first.org/cvss/
[5] https://cwe.mitre.org
[6] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CVE ID: CVE-2026-107408

Published: 2026-11-12

Vendor: Citrix NetScaler

Product: ADC

CVSS Score[7]: 9.3

Common Weakness Enumeration (CWE)[8]: CWE-787

Known Exploited Vulnerability (KEV) catalog[9]: No

Used by Ransomware Operators: N/A

CVE ID: CVE-2026-107409

Published: 2026-11-12

Vendor: Citrix NetScaler

Product: NetScaler

CVSS Score[10]: 9.3

Common Weakness Enumeration (CWE)[11]: CWE-415

Known Exploited Vulnerability (KEV) catalog[12]: No

Used by Ransomware Operators: N/A

[7] https://www.first.org/cvss/
[8] https://cwe.mitre.org
[9] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[10] https://www.first.org/cvss/
[11] https://cwe.mitre.org
[12] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CVE ID: CVE-2026-107410

Published: 2026-11-12

Vendor: Citrix NetScaler

Product: Netscaler

CVSS Score[13]: 9.3

Common Weakness Enumeration (CWE)[14]: CWE-122

Known Exploited Vulnerability (KEV) catalog[15]: No

Used by Ransomware Operators: N/A

CVE ID: CVE-2026-107412

Published: 2026-11-12

Vendor: Citrix NetScaler

Product: Gateway

CVSS Score[16]: 9.5

Common Weakness Enumeration (CWE)[17]: CWE-119

Known Exploited Vulnerability (KEV) catalog[18]: No

Used by Ransomware Operators: N/A

[13] https://www.first.org/cvss/
[14] https://cwe.mitre.org
[15] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[16] https://www.first.org/cvss/
[17] https://cwe.mitre.org
[18] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CVE ID: CVE-2026-107415

Published: 2026-11-12

Vendor: Citrix NetScaler

Product: ADC

CVSS Score[19]: 9.3

Common Weakness Enumeration (CWE)[20]: CWE-122

Known Exploited Vulnerability (KEV) catalog[21]: No

Used by Ransomware Operators: N/A

CVE ID: CVE-2026-111334

Published: 2026-11-12

Vendor: Citrix NetScaler

Product: Netscaler

CVSS Score[22]: 9.5, 9.3

Common Weakness Enumeration (CWE)[23]: CWE-119

Known Exploited Vulnerability (KEV) catalog[24]: No

Used by Ransomware Operators: N/A

[19] https://www.first.org/cvss/
[20] https://cwe.mitre.org
[21] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[22] https://www.first.org/cvss/
[23] https://cwe.mitre.org
[24] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CVE ID: CVE-2026-120864.

Published: 2026-11-12

Vendor: Citrix NetScaler

Product: Netscaler

CVSS Score[25]: 9.3

Common Weakness Enumeration (CWE)[26]: CWE-119

Known Exploited Vulnerability (KEV) catalog[27]: No

Used by Ransomware Operators: N/A

[25] https://www.first.org/cvss/

[26] https://cwe.mitre.org

[27] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

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 NetScaler.

- https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697305
- https://community.citrix.com/techzone-blogs/110_security-updates/security-updates-for-netscaler-adc-netscaler-gateway-and-netscaler-console/