An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2608170215

NCSC Advisory

NetScaler: Gateway, ADC

CVE-2026-8452

17 August 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-2026-8452

Published: 2026-06-30

Vendor: NetScaler

Product: Gateway, ADC

CVSS Score[1]: 8.8

Products Affected

Product	Version
ADC	14.1 < 14.1-72.61
ADC	13.1 < 13.1-63.18
ADC	14.1 FIPS < 14.1-72.61
ADC	13.1 FIPS and NDcPP < 13.1-37.272
Gateway	14.1 < 14.1-72.61
Gateway	13.1 < 13.1-63.18

Impact

A memory overflow vulnerability in NetScaler ADC and NetScaler Gateway may allow an unauthenticated remote attacker to cause a denial of service when the appliance is configured as a Gateway (SSL VPN, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server.

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

Known Exploited Vulnerability (KEV) catalog[3]: 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

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 NetScaler.

- https://nvd.nist.gov/vuln/detail/CVE-2026-8452
- https://www.cve.org/CVERecord?id=CVE-2026-8452
- https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604