CERT-EU

Security Advisory 2026-020

Critical Vulnerabilities in Citrix NetScaler ADC and NetScaler Gateway

2026-11-12 — v1.0

TLP:CLEAR

History:

- *12/11/2026 — v1.0 – Initial publication*

Summary

On 12 November 2026, the Cloud Software Group published security bulletins for its **Citrix** products addressing 28 memory flaws in **Citrix NetScaler ADC** and **Citrix NetScaler Gateway** [1, 2]. One of these vulnerabilities, **CVE-2026-120868**, affects every deployment, including those using the default configuration [2]. The vendor bulletin describes the impact as unpredictable behaviour and denial of service [2].

Citrix reports no exploitation, and no public proof-of-concept has been confirmed [1]. CERT-EU strongly recommends upgrading all customer-managed NetScaler ADC and NetScaler Gateway appliances to the fixed releases. Internet-facing Gateway and AAA appliances should be upgraded first.

Technical Details

The vulnerability **CVE-2026-120868**, with a CVSS score of 9.3, is a memory overflow vulnerability in core packet processing that does not require any special feature or authentication. The NetScaler ADC and Gateway bulletin states that all deployments are affected, including those with the default configuration [2].

The vulnerability **CVE-2026-107412**, with a CVSS score of 9.5, covers several memory overflow vulnerabilities that affect appliances configured as a Gateway (SSL VPN, ICA Proxy, CVPN or RDP Proxy) or as an AAA virtual server. According to the vendor, these issues can be reached without authentication [2].

The remaining vulnerabilities depend on specific features, including SAML, WebAuth, LDAP, Email OTP and client-certificate authentication. Others affect DNS-over-HTTPS, HTTP/2, HTTP/3 (QUIC), SMPP, RTSP, BGP routing and the Application Firewall. Ten of the flaws are scored as having a high impact on confidentiality, integrity and availability. However, the vendor bulletin describes their impact only as unpredictable behaviour or denial of service [2].

Affected Products

The following versions of Citrix NetScaler ADC and Citrix NetScaler Gateway are affected:

- 14.1 before 14.1-73.57
- 13.1 before 13.1-64.39
- NetScaler ADC FIPS before 14.1-73.58 FIPS
- NetScaler ADC FIPS and NDcPP before 13.1-37.293

Additional information is available in the vendor's advisory [2].

Recommendations

CERT-EU strongly recommends upgrading all affected appliances to the fixed releases prioritising internet-facing Gateway and AAA appliances.

References

[1] https://community.citrix.com/techzone-blogs/110_security-updates/security-updates-for-netscaler-adc-netscaler-gateway-and-netscaler-console/

[2] https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697305