GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

18 November 2026

Advisory 385: Citrix NetScaler ADC, NetScaler Gateway and NetScaler Console Multiple Vulnerabilities (CVE-2026-120868, CVE-2026-120869 and others).

Release Date: 13th November 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

On 12 November 2026, Citrix published security bulletin CTX697305, fixing 28 memory safety vulnerabilities in NetScaler ADC and NetScaler Gateway, and bulletin CTX697320, fixing an authentication bypass in NetScaler Console. Most of the NetScaler flaws can cause unpredictable behaviour or denial of service, and many can be reached over the network without logging in.

The most serious is CVE-2026-120868 (CVSS v4.0 9.3), a memory overflow in packet processing that affects every NetScaler ADC and Gateway deployment, including the default configuration. CVE-2026-107412 (CVSS 9.5) affects appliances configured as a Gateway (SSL VPN, ICA Proxy, CVPN or RDP Proxy) or AAA virtual server. CVE-2026-120869 (CVSS 9.4) in NetScaler Console allows an unauthenticated attacker to bypass authentication and access restricted resources.

What are the systems affected?

The vulnerabilities affect:

- NetScaler ADC and NetScaler Gateway 14.1 before 14.1-73.57
- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-64.39

- NetScaler ADC 14.1-FIPS before 14.1-73.58 FIPS, and 13.1-FIPS and 13.1-NDcPP before 13.1-37.293
- NetScaler Console before 14.1-74.34
- Unsupported releases such as 12.1 and 13.0 are end of life and will not be fixed

Not affected / patched version:

- NetScaler ADC and Gateway 14.1-73.57, 13.1-64.39, 14.1-73.58 FIPS or 13.1-37.293 FIPS/NDcPP, or later
- NetScaler Console 14.1-74.34 or later

What does this mean?

Successful exploitation may allow attackers to:

- Crash NetScaler appliances and cut off remote access and published applications
- Cause unpredictable behaviour that may be developed into code execution, as seen with earlier NetScaler memory flaws
- Access restricted NetScaler Console resources without logging in, and from there the appliances it manages

Mitigation process

CERTVU recommends the following:

1. Upgrade NetScaler ADC and Gateway
Upgrade to the fixed builds listed above, starting with internet-facing Gateway and AAA appliances. Appliances updated to the builds recommended in Advisories 336, 342 or 353 must be updated again.

2. Upgrade NetScaler Console
3. Replace end-of-life appliances
4. Monitor for exploitation

Report incidents to CERTVU at incident@cert.gov.vu.

Reference

1. https://support.citrix.com/external/article/CTX697305
2. https://support.citrix.com/external/article/697320
3. https://www.cve.org/CVERecord?id=CVE-2026-120868
4. https://www.cve.org/CVERecord?id=CVE-2026-120869
5. https://cyber.gc.ca/en/alerts-advisories/citrix-security-advisory-av26-1150