

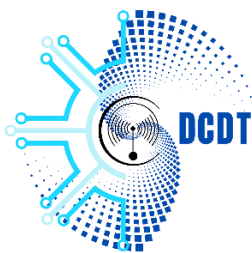
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

7 September 2026

Advisory 262: Citrix NetScaler ADC and NetScaler Gateway Memory Overflow and Authentication Bypass (CVE-2026-19489, CVE-2026-19490).

Release Date: 4th September 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 utilise Citrix NetScaler ADC and/or NetScaler Gateway products. This alert is intended for a technical audience.

What is it?

Citrix has disclosed two vulnerabilities affecting NetScaler ADC and NetScaler Gateway, critical edge devices that organisations use to securely deliver applications, data, and remote access to users, and which are frequently targeted by threat actors as an entry point into sensitive environments. CVE-2026-19489 is a memory overflow vulnerability that requires SIP ALG (Session Initiation Protocol Application Layer Gateway) to be enabled on a Large Scale NAT (LSN) group configuration, and can lead to unpredictable device behaviour or denial of service.

What are the systems affected?

The following version(s) are affected:

- NetScaler ADC and NetScaler Gateway 14.1 before 14.1-73.32 - (Affected)
- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-63.21 - (Affected)

NetScaler ADC FIPS/NDcPP before 14.1-73.32 FIPS and before 13.1-37.277, and all versions 13.1-FIPS and 12.1 (both end-of-life) - (Affected)

What does this mean?

Typical attack flow:

1. **CVE-2026-19489: trigger the memory overflow via SIP traffic**
 - On a NetScaler configured with SIP ALG enabled on a Large Scale NAT (LSN) group, a remote, unauthenticated attacker sends crafted SIP traffic that overflows a memory buffer, causing unpredictable device behaviour or a denial-of-service condition.
2. **CVE-2026-19490: bypass authentication via an alternate path**
 - On a NetScaler configured as a Gateway (SSL VPN, ICA Proxy, CVPN, or RDP Proxy virtual server) or as an AAA virtual server, with SAML actions configured in some affected versions, a remote, unauthenticated attacker reaches an alternate request path that bypasses the intended authentication check entirely, gaining access without presenting valid credentials.

Attack vectors:

- A network-based, unauthenticated attack against any internet- or network-reachable NetScaler ADC or NetScaler Gateway instance running an affected version with the relevant configuration enabled (SIP ALG on an LSN group for CVE-2026-19489; Gateway or AAA virtual server configuration for CVE-2026-19490).
- No user interaction and no privileges are required for either vulnerability. Rapid7 had not observed active exploitation as of 19 August 2026 and CERTVU found no subsequent report of confirmed active exploitation, but NetScaler devices are high-value, internet-facing targets that have historically seen rapid exploitation once a vulnerability of this kind becomes public.

Successful exploitation may allow attackers to:

- Cause unpredictable behaviour or denial of service on an affected NetScaler device via CVE-2026-19489, disrupting the application delivery and remote-access services it provides.
- Bypass authentication entirely via CVE-2026-19490 and gain unauthorized access to the NetScaler Gateway or AAA virtual server — and, from there, to the applications, data, and internal network resources the device was deployed to protect — without ever presenting valid credentials.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch as a priority

- Update NetScaler ADC and NetScaler Gateway to 14.1-73.32 or later, or 13.1-63.21 or later (including the corresponding FIPS/NDcPP builds), per Citrix Security Bulletin CTX696939. Devices still on end-of-life 12.1 or 13.1-FIPS must be upgraded to a supported, fixed version, as no patch will be issued for those releases.

2. Treat this as urgent: critical edge devices like NetScaler are frequently and rapidly targeted by threat actors once a vulnerability is disclosed
3. Assess the environment for the specific vulnerable configurations
4. Confirm third-party-managed instances have been patched
5. Review the vendor's own mitigation advice and monitor for suspicious activity

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://support.citrix.com/external/article/CTX696939/netscaler-adc-and-netscaler-gateway-secu.html>
2. <https://www.cve.org/CVERecord?id=CVE-2026-19489>
3. <https://www.cve.org/CVERecord?id=CVE-2026-19490>