

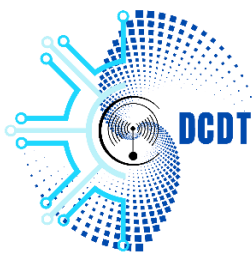
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

12 October 2026

**Advisory 353: Citrix NetScaler ADC and Gateway SAML Memory Overflow
Remote Code Execution Vulnerability (CVE-2026-107406).**

Release Date: 9th October 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?

CVE-2026-107406 is a critical memory overflow vulnerability (CWE-119) in Citrix NetScaler ADC and NetScaler Gateway that can lead to remote code execution or denial of service when the appliance is configured as a SAML identity provider (IdP) or SAML service provider (SP). It is rated CVSS v4.0 9.5. It needs no authentication or user interaction, although the attack complexity is rated high.

What are the systems affected?

Only appliances configured for SAML authentication are affected, either as an identity provider ("authentication samlIdPProfile") or a service provider ("authentication samlAction"). The following builds are affected:

- SAML IdP only: NetScaler ADC and Gateway 14.1-73.37 through 14.1-73.41 and 13.1-64.23 through 13.1-64.28, including the FIPS builds 14.1-73.37 FIPS through 14.1-73.41 FIPS and 13.1-FIPS/NDcPP 13.1-37.279 through 13.1-37.282
- SAML IdP or SP: any build before 14.1-73.37, and any build before 13.1-64.23 (13.1-FIPS/NDcPP before 13.1-37.279)

- Secure Private Access hybrid deployments that use NetScaler. Citrix-managed cloud services and Adaptive Authentication are not affected

Citrix lists no workaround. End-of-life releases receive no fix and must be migrated to a supported branch.

Not affected / patched version:

- NetScaler ADC and Gateway 14.1-73.46 or later, and 13.1-64.29 or later
- NetScaler ADC 14.1-FIPS 14.1-73.46 FIPS or later, and 13.1-FIPS/NDcPP 13.1-37.283 or later

What does this mean?

Successful exploitation may allow attackers to:

- Cause memory corruption on the NetScaler by sending crafted requests to a SAML virtual server, without credentials
- Run code on the appliance, or crash it and cut off VPN, single sign-on and gateway access for users
- Take control of a device at the network edge that handles authentication, and use it to capture credentials, hijack sessions and move into the internal network

Mitigation process

CERTVU recommends the following:

1. Upgrade to the new fixed builds

Upgrade to 14.1-73.46 or later, 13.1-64.29 or later, or the fixed FIPS/NDcPP build above. Do this even if the appliance was patched in September 2026, because those builds remain affected when SAML IdP is used.

2. Identify SAML configurations

3. Remove SAML where it is not needed

4. Replace unsupported appliances

Identify end-of-life NetScaler appliances. They receive no fix and must be migrated to a supported release.

5. Monitor and investigate

Review logs for crashes or restarts of SAML virtual servers and for abnormal requests to authentication endpoints, apply the indicators of compromise in Advisories 336 and 342, and report suspected compromise to CERTVU.

Reference

1. <https://thehackernews.com/2026/10/citrix-patches-critical-netscaler-flaw.html>
2. <https://www.itnews.com.au/news/netscaler-builds-that-fixed-zero-days-carry-critical-flaw-too-629542>
3. <https://cycognito.com/blog/emerging-threat-cve-2026-107406-netscaler-adc-and-gateway-remote-code-execution-via-saml-2>
4. <https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/critical-vulnerabilities-in-citrix-netscaler-adc-and-citrix-netscaler-gateway-products>
5. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>