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

27 August 2026

Advisory 202: CVE-2026-8452 - Citrix NetScaler ADC and NetScaler Gateway Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Release Date: 26th August 2026
Impact: CRITICAL
TLP: CLEAR

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

Any organisation using Citrix NetScaler ADC or NetScaler Gateway to provide remote access, load balancing or single sign-on. In Vanuatu this is most likely to apply to banking and financial institutions, telecommunications operators and Internet Service Providers, government agencies providing staff remote access, and larger private sector organisations.

What is it?

CVE-2026-8452 is a memory overflow vulnerability (CWE-119) in Citrix NetScaler ADC and NetScaler Gateway, carrying a CVSS v4.0 Base Score of 8.8. It can be triggered by a remote, unauthenticated attacker with no user interaction, using a single HTTP request to an affected virtual server.

Citrix published the vulnerability on 30 June 2026 in security bulletin CTX696604, alongside five other issues, describing it as a memory overflow leading to unpredictable or erroneous behaviour and denial of service.

CERTVU draws attention to the fact that subsequent independent research has established the practical impact to be materially greater than the vendor description indicates the appliance.

What are the systems affected?

NetScaler ADC and NetScaler Gateway, 13.1 and 14.1 branches, on builds prior to those listed as fixed in Citrix bulletin CTX696604 - (Affected)

Builds listed as fixed in CTX696604, or later - (Not affected, patched)

Organisations should confirm exact affected and fixed build numbers against CTX696604 directly, as Citrix maintains the authoritative version matrix. Appliances not configured as a Gateway or AAA virtual server are not exploitable through this path.

What does this mean?

NetScaler Gateway appliances sit at the network perimeter, are internet-facing by design, terminate remote access sessions, and hold or broker the credentials of every user who connects through them. Appliances of this class have been among the most heavily targeted initial access points in recent years, and are routinely exploited by ransomware operators and state-sponsored actors to obtain entry into corporate and government networks.

Mitigation process

CERTVU recommends the following:

1. **Identify Affected Virtual Servers**

Determine whether any appliance is configured as a Gateway or AAA virtual server, and whether SAML authentication is in use, by inventorying the configured virtual servers on each appliance.

```
show authentication vserver
show vpn vserver
```

2. **Upgrade Without Delay**

Upgrade affected appliances to a fixed 13.1 or 14.1 build as listed in Citrix bulletin CTX696604. Given that the vulnerability is pre-authentication, reachable from the internet, and supported by public proof-of-concept tooling, CERTVU recommends treating this as an emergency change rather than a scheduled one.

Other mitigating options include;

- Confirm the Upgrade Took Effect
- Restrict Exposure Where Upgrade Is Delayed
- Assume Compromise and Review

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

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-8452
2. https://nvd.nist.gov/vuln/detail/CVE-2026-8452
3. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

4. https://docs.netscaler.com/en-us/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2026-8452.html
5. https://cwe.mitre.org/data/definitions/119.html