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 386: Citrix Secure Access Client Improper Privilege Management Vulnerabilities (CVE-2026-118268 and CVE-2026-118269).

Release Date: 17th November 2026
Impact: HIGH
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 fixed two improper privilege management vulnerabilities in the Citrix Secure Access Client, the VPN client used to connect to NetScaler Gateway. Each is rated CVSS 8.5 (High). A low-privileged user on a computer with the client installed can escalate their privileges to full control of the computer.

- CVE-2026-118268 (Windows): a low-privileged user can gain SYSTEM privileges (bulletin CTX697280)
- CVE-2026-118269 (Linux): a low-privileged user can gain root privileges (bulletin CTX697281)

What are the systems affected?

The vulnerabilities affect:

- Citrix Secure Access Client for Windows before 26.11.1.6
- Citrix Secure Access Client for Linux before 26.10.4

Not affected / patched version:

- Citrix Secure Access Client for Windows 26.11.1.6 or later
- Citrix Secure Access Client for Linux 26.10.4 or later

What does this mean?

Successful exploitation may allow attackers to:

- Take full control of the user's computer
- Disable security tools and install persistent malware
- Steal credentials, including VPN and domain credentials stored on the device

Mitigation process

CERTVU recommends the following:

1. Update the client
Update the Secure Access Client on all Windows and Linux computers to the fixed versions. Where the client is deployed from NetScaler Gateway, update the client package published on the Gateway so users receive the fixed version.

2. Limit local privileges
3. Monitor endpoints

Report suspected compromise to CERTVU at incident@cert.gov.vu.

Reference

1. https://support.citrix.com/external/article/CTX697280
2. https://support.citrix.com/external/article/CTX697281
3. https://www.cve.org/CVERecord?id=CVE-2026-118268
4. https://www.cve.org/CVERecord?id=CVE-2026-118269