**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 380: SonicWall SonicOS SSLVPN SAML and MFA Bypass Vulnerability (CVE-2026-19868).

**Release Date:** 10th 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?

CVE-2026-19868 is an authentication enforcement vulnerability (CWE-308) in the SSLVPN service of SonicOS, the operating system of SonicWall firewalls. When SAML is enabled for SSLVPN logins, a user with valid credentials for another login method can bypass SAML authentication controls, and with them any multi-factor authentication (MFA) enforced through SAML.

# What are the systems affected?

The vulnerability affects SonicWall firewalls with SAML enabled for SSLVPN logins, running:

- Gen 7 firewalls and NSv virtual appliances: SonicOS 7.3.3-7015 and earlier
- Gen 8 firewalls: SonicOS 8.2.2-8015 and earlier

Not affected / patched version:

- Gen 7: SonicOS 7.3.4-7013 or later
- Gen 8: SonicOS 8.2.3-8015 or later
- Firewalls that do not use SAML for SSLVPN logins are not affected by this CVE, but should still be updated for the other six flaws in the advisory

# What does this mean?

Successful exploitation may allow attackers to:

- Log in to the SSLVPN with stolen credentials without passing MFA
- Gain remote access to internal networks behind the firewall
- Move laterally, steal data or deploy ransomware

# Mitigation process

CERTVU recommends the following:

1. Upgrade SonicOS
Upgrade Gen 7 firewalls to SonicOS 7.3.4-7013 or later and Gen 8 firewalls to SonicOS 8.2.3-8015 or later. SonicWall lists no workaround.

2. Check whether SAML is used for SSLVPN
3. Reset credentials and review accounts
4. Check for compromise

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

# Reference


1. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0014
2. https://www.cve.org/CVERecord?id=CVE-2026-19868
3. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-19868