KILLSWITCH · ISSUE #19 · 20 NOV 2026

MFA Was a Second Door: The SonicWall SSLVPN Path That Skipped SAML

Valid credentials on an alternate SSLVPN login method could skip SAML, and may also skip SAML-enforced MFA.

Killswitch rating: Inventory every SSLVPN login path

By Emmanuel Aigbehi Walstra

MFA was a second door

A SonicWall SSLVPN flaw lets valid credentials on an alternate login method bypass SAML controls, and may also bypass SAML-enforced MFA [2][3][5].

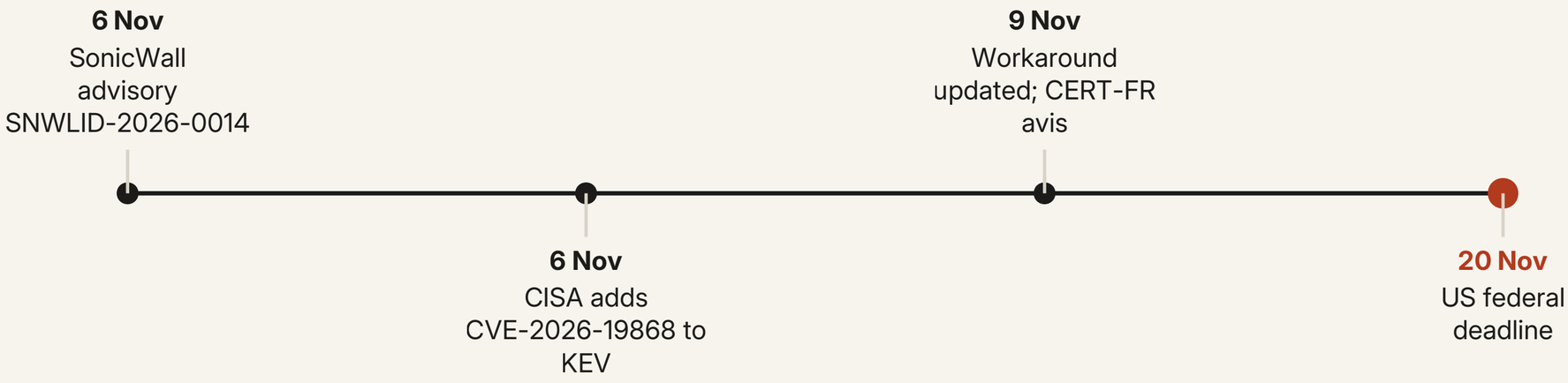
- CISA added CVE-2026-19868 to KEV on 6 November, with a US federal deadline of 20 November [1][2].
- "MFA is on" is not evidence that every login path requires it.

Exploited, due 20 November

- CVE-2026-19868, SonicWall SonicOS SSLVPN [2][3][5].
- Vendor CVSS 3.1: 7.1; CISA ADP on NVD: 7.5 [3][5].
- CISA: known exploited; forensic triage not required; ransomware use "Unknown" [2]. SonicWall: its PSIRT has investigated a report indicating potential exploitation [5].
- Fixed in SonicOS 7.3.4-7013 and higher (Gen7) and 8.2.3-8015 and higher (Gen8) [5].

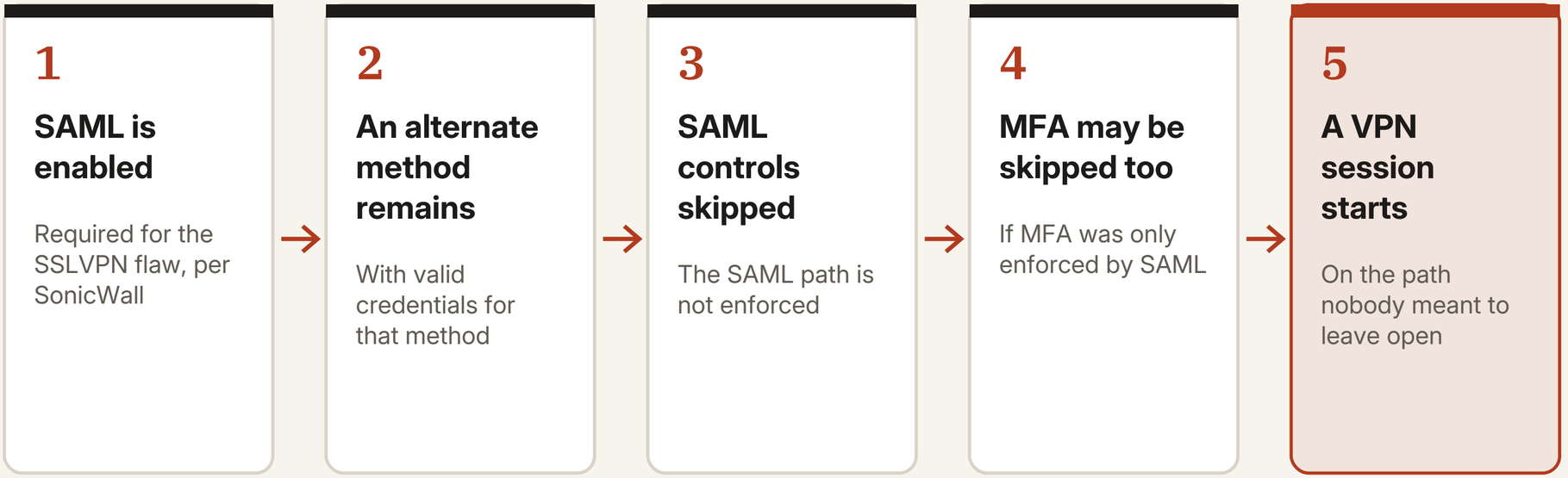
03 · TIMELINE

From the advisory to the federal deadline



SonicWall [5]: first published 6 November, workaround updated 9 November. CISA [1][2] added the CVE on 6 November. All dates 2026.

How an alternate login skipped SAML



Described from CISA, NVD and SonicWall [2][3][5], at design level only. SonicWall: the flaw affects SSLVPN only if SAML is enabled for SSLVPN logins.

The unused path was still a path

- SonicWall: the flaw affects SSLVPN only if SAML is enabled for SSLVPN logins [5].
- The intended path is SAML, often with MFA attached to it [2][3][5].
- An alternate method with valid credentials could skip the SAML controls [2][3][5].
- If MFA was only enforced by SAML, it may have been skipped too [2][3][5].

SSLVPN with SAML, and another method still on

- SonicWall says the flaw affects SSLVPN only if SAML is enabled for SSLVPN logins [5].
- Affected: SonicOS 7.3.3-7015 and older (Gen7) and 8.2.2-8015 and older (Gen8) [5].
- You are in scope if SAML is enabled for SSLVPN and an alternate method can still succeed [2][3][5].

07 · RESPOND

Six moves, in this order

1 Inventory

Every SSLVPN authentication method still enabled

2 Make SAML the only path

Disable or remove every alternate method that can still succeed

3 Apply the vendor patches

SonicOS 7.3.4-7013+ (Gen7) and 8.2.3-8015+ (Gen8)

4 If you cannot upgrade yet

Disable or delete active LDAP, RADIUS and TACACS+ servers, if SAML is in use

5 Confirm MFA is enforced

"MFA is on" is not evidence that every path requires it

6 Watch for odd logins

Successful SSLVPN sessions that did not use SAML

Fixed versions and workaround: SonicWall SNWLID-2026-0014 [5]. The inventory and the "MFA is on is not evidence" test are Killswitch additions.

Where this lives in your frameworks

Remote access and MFA	A.5.15, A.8.5, A.5.17 · NIS2 21(2)(i), (j) · Evidence: the list of SSLVPN methods and which ones enforce MFA
Patch	A.8.8, A.8.32 · NIS2 21(2)(e) · Evidence: version record and patch date from the vendor advisory
Detect	A.8.15, A.8.16 · NIS2 21(2)(b) · Evidence: SSLVPN login logs reviewed for non-SAML successes
Suppliers	A.5.19, A.5.21 · NIS2 21(2)(d) · Evidence: if an MSP runs the firewall, their patch and method inventory

Killswitch's own mapping. Check ISO titles against your licensed copy.

ISO/IEC 27001:2022 [6] · NIS2 Art. 21(2), Art. 23 [7]. Killswitch mapping.

09 · STILL OPEN

What we don't know yet

- No victim, actor or scale is public; KEV ransomware use: "Unknown" [1][2].
- LDAP, RADIUS and TACACS+ are named as workaround targets, not as a complete list of alternate methods [5].

This week

- Inventory every SSLVPN authentication method [2][3][5].
- Disable every alternate method if SAML and MFA are the intended path.
- Apply SonicOS 7.3.4-7013+ (Gen7) or 8.2.3-8015+ (Gen8) [5].
- If you cannot upgrade, disable or delete active LDAP, RADIUS and TACACS+ servers when SAML is in use [5].
- Review non-SAML SSLVPN successes. Keep a short record of the patch or workaround.

Sources

[1] CISA: CISA Adds One Known Exploited Vulnerability to Catalog (6 Nov 2026)
[2] CISA: Known Exploited Vulnerabilities Catalog, CVE-2026-19868 (added 6 Nov 2026, due 20 Nov 2026)
[3] NIST NVD: CVE-2026-19868 (published 6 Nov 2026)
[4] CERT-FR: Avis CERTFR-2026-AVI-1483, Multiples vulnérabilités dans Sonicwall SonicOS (9 Nov 2026)
[5] SonicWall: Security advisory SNWLID-2026-0014 (published 6 Nov 2026, updated 9 Nov 2026)
[6] ISO/IEC 27001:2022 Information security management systems
[7] NIS2 Directive (EU) 2022/2555, Articles 21 and 23

Facts are from CISA's 6 November alert and KEV entry, the NVD record, CERT-FR's 9 November avis, and SonicWall advisory SNWLID-2026-0014 (published 6 November, updated 9 November), as published by 20 Nov 2026. The framework mapping, the inventory control and the tabletop are Killswitch's own.

FROM THE PUBLISHERS OF KILLSWITCH

Know every remote-access login path, and which one actually enforces MFA

GRCOMPLIANCE

Keep an inventory of remote-access authentication methods and their evidence, and map the controls to ISO 27001 and NIS2.

Try the live demo →

demo.grcompliance.com

Self-host free: github.com/Sectutor/GRCompliance-Core

SECTUTOR

Security and GRC books, training and audit kits.

sectutor.com

Emmanuel Aigbehi Walstra is a CISO who also serves as a virtual CISO (vCISO) for several organisations, with 30+ years in cybersecurity, 10,000+ people trained, and author of the CCSP Excellence books.