Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-19868: SonicOS Vulnerability Exploited in the Wild

Date of Publication	Admiralty Code	TA Number
November 09, 2026	A1	TA2026328

Summary

First Seen: November 6, 2026
Affected Products: SonicWall SonicOS SSLVPN - Gen7 (7.3.3-7015 and older) and Gen8 (8.2.2-8015 and older)
Impact: CVE-2026-19868 is an authentication flaw in SonicWall SonicOS SSLVPN. When SAML authentication is required, the VPN still accepts logins through other authentication methods configured on the device, so an attacker with one valid password can open a VPN session that never passes the identity provider's policy or MFA. The flaw is being exploited in the wild, and CISA has added it to its Known Exploited Vulnerabilities catalog with a November 20, 2026 remediation deadline. Once inside, attackers can move laterally, steal data, or stage ransomware while leaving little identity-provider telemetry behind. Organizations running affected SonicOS versions should apply SonicWall's fixes or mitigations immediately.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-19868	SonicWall SonicOS SSLVPN Use of Single-factor Authentication Vulnerability	SonicWall SonicOS SSLVPN	✓	✓	✓

Vulnerability Details

#1

CVE-2026-19868 is classified as CWE-308 (Use of Single-factor Authentication). When SonicOS SSLVPN is configured to require SAML authentication, the service still accepts logins through other authentication methods configured on the device. As a result, the SAML requirement, and any MFA enforced through it, is not applied consistently, and the protection of the VPN falls back to a single password. Organizations that use SAML single sign-on to secure SSLVPN access are the ones exposed, since they rely on the identity provider to enforce login policy.

#2

To exploit the flaw, an attacker connects to the internet-facing SSLVPN portal and logs in using valid credentials for one of these alternate methods. No prior access to the device or action by a legitimate user is required. The result is an authenticated VPN session that never passed through SAML or MFA, and that is therefore invisible to the conditional access, device checks, and sign-in monitoring configured at the identity provider. Obtaining valid credentials is the main hurdle, but such credentials are widely available to attackers through phishing, infostealer malware, and password reuse.

#3

CISA rates the vulnerability 7.5 (High) on the CVSS v3.1 scale. The rating reflects a network-based attack that needs no privileges or user interaction, offset by higher attack complexity because valid credentials are required. A successful attack reaches beyond the firewall itself to the internal resources the VPN exposes, with a high impact on confidentiality, a limited impact on integrity, and no direct impact on availability. In practice, this makes the flaw a tool for quiet access and data theft rather than disruption.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-19868	SonicWall SonicOS SSLVPN Gen7 (7.3.3-7015 and older), Gen8 (8.2.2-8015 and older)	cpe:2.3:o:sonicwall:sonicos:*:*:*:*:*:*:*:*	CWE-308

Recommendations

Apply the SonicWall Fixed Release: Upgrade every affected Gen7 and Gen8 firewall to the fixed SonicOS release listed in SonicWall advisory SNWLID-2026-0014, and confirm the full version string after the upgrade. Prioritize internet-facing devices and complete the update within the CISA KEV timeline.

Enforce SAML as the Only SSLVPN Login Path: Where SAML is the intended authentication method for remote access, remove or disable local, LDAP, RADIUS, and other alternate authentication methods for SSLVPN users. Every remaining login path should require MFA, so that no single password can grant VPN access on its own.

Reduce SSLVPN Exposure: Limit who can reach the SSLVPN portal by restricting access to known source IP ranges or countries where the business operates, and disable SSLVPN on devices that do not need it. A smaller attack surface leaves less room for credential-based attacks.

Harden Credentials on the Appliance: Remove stale and unused local accounts, enforce strong unique passwords for any account the VPN accepts, and check corporate credentials against breach and infostealer exposure sources. Exploitation depends on valid credentials, so shrinking and protecting that pool directly lowers the risk.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1133: External Remote Services	
	T1078: Valid Accounts	
Defense Impairment	T1556: Modify Authentication Process	T1556.006: Multi-Factor Authentication
Persistence	T1133: External Remote Services	
Credential Access	T1110: Brute Force	T1110.004: Credential Stuffing
Lateral Movement	T1021: Remote Services	

Patch Link

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0014

References

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0014

https://github.com/advisories/GHSA-mq8w-j7h6-7q9w

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

November 09, 2026 • 11:30 PM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com