BLACKSWAN CYBERSECURITY

THREAT ADVISORY

September 10, 2024

SonicWall Firewall Vulnerability

SUMMARY

SonicWall's self-disclosed critical security vulnerability in SonicOS is now under active exploitation. Available updates should be applied as soon as possible. The vulnerability (CVE-2024-40766) has a CVSS score of 9.3 out of 10 and stems from improper access control in the SonicOS management interface and SSLVPN, which could allow unauthorized access to resources and, under certain conditions, trigger a firewall crash.

TECHNICAL DETAILS

CVE-2024-40766 is a critical access control vulnerability with a CVSS v3 score of 9.3, affecting multiple generations of SonicWall Firewall devices, including Gen 5, Gen 6, and Gen 7 models. The flaw, initially disclosed on August 22, 2024, affects the management interface of SonicOS, but recent updates indicate it also impacts the SSLVPN feature. The vulnerability could allow unauthorized resource access and may also lead to firewall crashes.

AFFECTED DEVICES AND VERSIONS

- SonicWall Gen 5 running SonicOS version 5.9.2.14-12o and older: Fixed in SonicOS version 5.9.2.14-13o.
- SonicWall Gen 6 running SonicOS version 6.5.4.14-109n and older: Fixed in 6.5.2.8-2n (for SM9800, NSsp 12400, NSsp 12800) and 6.5.4.15-116n (for other Gen 6 firewalls).
- SonicWall Gen 7 running SonicOS version 7.0.1-5035 and older: The issue is not reproducible in version 7.0.1-5035 and later.

SonicWall has not provided detailed technical information on how the vulnerability is exploited but highlights its potential to allow unauthorized access and cause firewall failures, which could leave corporate networks exposed. Given that SonicWall firewalls are often accessible via the internet for VPN services, they are prime targets for exploitation.

RECOMMENDATIONS

SonicWall's critical steps for securing devices against CVE-2024-40766.

- Restrict SonicOS management portal access to trusted sources only. Disabling internet access to the WAN management portal entirely can significantly reduce exposure.
- Only allow SSLVPN access from trusted sources. If SSLVPN functionality is not required, disable it to further reduce attack surface.
- For Gen 5 and Gen 6 devices, administrators should enforce immediate password changes for SSLVPN users with local accounts. The "User must change password" option should also be enabled for all local users.
- Activate MFA for all SSLVPN users to add an additional layer of security. SonicWall supports MFA using Time-based One-Time Passwords (TOTP) or email-based OTPs, providing stronger protection against unauthorized access. Detailed configuration instructions for MFA are available on SonicWall's support portal.
- Ensure that all affected devices are running the latest patched firmware versions as outlined above. Regularly check for firmware updates and apply them promptly to mitigate known vulnerabilities.

REFERENCES

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015
- https://www.sonicwall.com/support/knowledge-base/how-do-i-configure-2fa-for-ssl-vpn-with-totp/190829123329169
- https://thehackernews.com/2024/09/sonicwall-urges-users-to-patch-critical.html

- https://www.bleepingcomputer.com/news/security/sonicwall-sslvpn-access-control-flaw-is-now-exploited-in-attacks/