Health-ISAC™
Collaborating for Resilience in Healthcare

THREAT BULLETINS

SonicWall SonicOS Flaw Confirmed to be Exploited In-the-Wild After PoC Release

TLP:WHITE

Feb 19, 2025

The high-severity SSLVPN authentication bypass flaw affecting SonicWall firewalls running vulnerable SonicOS versions is actively being exploited in-the-wild. The exploitation activity follows the release of proof-of-concept exploit code by Bishop Fox.

On February 10, 2025, Bishop Fox researchers released proof-of-concept (PoC) exploit code for CVE-2024-53704 which affects SonicWall firewalls running SonicOS firmware versions 7.1.x (7.1.1-7058 and older), 7.1.2-7019, and 8.0.0-8035.
The vulnerability allows remote unauthenticated threat actors to hijack active SSL VPN client sessions. Successful exploitation can allow threat actors to view Virtual Office bookmarks, acquire NetExtender client configuration profiles, establish a VPN tunnel, access private networks accessible to the compromised account, and terminate the user's sessions.

According to Arctic Wolf security researchers, exploitation attempts targeting the security flaw were observed shortly after the PoC was made public. Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) recently added CVE-2024-53704 to its known exploited vulnerabilities (KEV) catalog, further confirming the

security flaw is being targeted in the threat landscape for successful intrusions.

Health-ISAC previously distributed an alert, Thousands of SonicWall Firewalls Face Imminent Risk of Exploitation, Patch Now to inform users about the matter before threat actors were observed exploiting the vulnerability. This alert is being released as an update to increase situational awareness and urge users to upgrade affected SonicWall infrastructure.

Recommendations:
Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and take the necessary actions to ensure appropriate security measures are enforced, including:

- Applying the patch as soon as possible to avoid exploitation.
- Ensuring access is limited to trusted sources or disabling SSLVPN access from the internet.
- Restricting firewall management to trusted sources or disabling firewall SSH management from internet access
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	Bishopfox, cisa, arcticwolf, SonicWall, NHS, Bleeping Computer, cybersecuritynews

Alert ID e47c1fce

View Alert

Share Feedback
was this helpful? |

Tags CVE-2024-53704, SonicWall

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments
Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**