CYBER ADVISORY

TLP:CLEAR
26 August 2024

SonicWall Vulnerability

CVE-2024-40766 | SonicWall | Improper Access | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-40766, with a reported CVSS v3 rating of 9.3.[1] The vulnerability affects multiple platforms of SonicWall Firewall Gen 5 and Gen 6 devices, as well as Gen 7 devices running SonicOS 7.0.1-5035 and older versions.[2] Exploitation of the improper access control vulnerability may allow an attacker unauthorized resource access and in specific conditions, causing the firewall to crash.[3]

Impacted Platforms	Impacted Versions
SOHO (Gen 5)	5.9.2.14-12o and older versions
Gen6 Firewalls -SOHOW, TZ 300, TZ 300W, TZ 400, TZ 400W, TZ 500, TZ 500W, TZ 600, NSA 2650, NSA 3600, NSA 3650, NSA 4600, NSA 4650, NSA 5600, NSA 5650, NSA 6600, NSA 6650, SM 9200, SM 9250, SM 9400, SM 9450, SM 9600, SM 9650, TZ 300P, TZ 600P, SOHO 250, SOHO 250W, TZ 350, TZ 350W	6.5.4.14-109n and older versions
Gen7 Firewalls - TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700,NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700	SonicOS build version 7.0.1-5035 and older versions. * However SonicWall recommends installation of the latest firmware.

Table 1: Impacted SonicWall Products

The Cal-CSIC recommends immediately upgrading to the appropriate fixed SonicWall version.

For further information on applying upgrades please refer to SonicWall Contact Support.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] The Hacker News; "SonicWall Issues Critical Patch for Firewall Vulnerability Allowing Unauthorized Access;" https://thehackernews.com/2024/08/sonicwall-issues-critical-patch-for.html; accessed 26 August 2024
[2] Cyber Scoop; "SonicWall pushes patch for critical vulnerability in SonicOS platform" https://cyberscoop.com/sonicwall-sonicos-firewall-cve-2024-40766/; accessed 26 August 2024
[3] SonicWall; "SonicOS Improper Access Control Vulnerability" https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015; accessed 26 August 2024