



CYBER ADVISORY



Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

TLP: CLEAR

9 January 2025

Multiple Vulnerabilities affecting SonicWall Products

- SonicWall
- CVE-2024-40762
- CVE-2024-53704
- CVE-2024-53705

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple vulnerabilities existing in SonicWall products ranging from Gen6 Hardware Firewalls, Gen7 Firewalls, Gen7 NSv, and TZ80.¹ SonicWall products deliver advanced network security by combining threat prevention, intrusion detection, and secure VPN access. These are designed to protect businesses from cyber threats while ensuring fast, reliable, and scalable connectivity.² Exploiting these cyber vulnerabilities could enable an attacker to execute remote code, bypass authentication, escalate privileges, and establish unauthorized remote connections. Currently, no Proof-of-Concepts are publicly available nor are there reported instances of these vulnerabilities being actively exploited.³

Additional details of each vulnerability can be found in the table below.

Affected Products	Issue	CVE (CVSS 3.1)
Gen6 Hardware Firewalls, Gen7 Firewalls, Gen7 NSv, and TZ80	Use of cryptographically weak pseudo-random number generator in the SonicOS SSLVPN authentication token generator that can be predicted by an attacker, potentially resulting in authentication bypass.	CVE-2024-40762 (7.1)
	An Improper authentication vulnerability in the SSLVPN authentication mechanism allows a remote attacker to bypass authentication.	CVE-2024-53704 (8.2)
	A server-side request forgery vulnerability in the SonicOS SSH management interface allows a remote attacker to establish a TCP connection	CVE-2024-53705 (6.5)

CAL-CSIC-202501-005

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP: CLEAR

PUBLIC SERVICE ANNOUNCEMENT

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

TLP:CLEAR

	to an IP address on any port when the user is logged in to the firewall.	
	A vulnerability in the Gen7 SonicOS Cloud platform NSv (AWS and Azure editions only), allows a remote authenticated local low-privileged attacker to elevate privileges to `root` and lead to code execution.	CVE-2024-53705 (7.8)

The Cal-CSIC recommends immediately updating to the latest SonicWall version for the affected products. Latest patch builds are available for [download](#).

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 here .
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	<i>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</i>

CAL-CSIC-202501-005

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP:CLEAR

PUBLIC SERVICE ANNOUNCEMENT

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

TLP:CLEAR

¹ Bleeping Computer; "SonicWall urges admins to patch exploitable SSLVPN bug immediately" <https://www.bleepingcomputer.com/news/security/sonicwall-urges-admins-to-patch-exploitable-sslvpn-bug-immediately/>; accessed 8 January 2025

² SonicWall; "Network Security Firewalls" <https://www.sonicwall.com/products/firewalls/>; accessed 8 January 2025

³ SonicWall; "Security Advisory Vulnerability List" <https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0003>; accessed 8 January 2025

CAL-CSIC-202501-005

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP:CLEAR