National Cyber Security Centre

2409060147-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability in SonicWall SonicOS; (CVE-2024-40766, CVSSv3: 9.3)

UPDATE - Version 1.2

Friday 13th September, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*
For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.
Please treat this document in accordance with the TLP assigned.

Revision History

Revision	Date	Author(s)	Description
1.0	06th September 2024	CSIRT-IE	Initial advisory
1.1	06th September 2024	CSIRT-IE	Update from SonicWall
1.2	13th September 2024	CSIRT-IE	Updated CVSS & EPSS Score & KEV information

Description

Published: 2024-08-23T07:15:00
Vendor: SonicWall
Product: SonicOS;
CVE ID: CVE-2024-40766
CVSS3.x Score[1]**:** 9.8
EPSS[2]**:** 0.841290000
(For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-40766)

Summary: An improper access control vulnerability has been identified in the SonicWall SonicOS management access, potentially leading to unauthorised resource access and in specific conditions, causing the firewall to crash. This issue affects SonicWall Firewall Gen 5 and Gen 6 devices, as well as Gen 7 devices running SonicOS 7.0.1-5035 and older versions.

This vulnerability is potentially being exploited in the wild. Please apply the patch as soon as possible for affected products.

Products Affected

This issue affects SonicWall Firewall Gen 5 and Gen 6 devices, as well as Gen 7 devices running SonicOS 7.0.1-5035 and older versions.

- **Impacted platform:** SOHO (Gen 5)
- **Impacted version:** 5.9.2.14-12o and older versions

- **Impacted platform:** 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
- **Impacted version:** 6.5.4.14-109n and older versions

- **Impacted platform:** 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;
- **Impacted version:** SonicOS build version 7.0.1-5035 and older versions.

Impact

Common Weakness Enumeration (CWE)[3]**:** CWE-284 Improper Access Control

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins
[3] https://cwe.mitre.org/

Present in CISA Known Exploited Vulnerability(KEV)[4] catalog: NO

Used by Ransomware Operators: Not Known

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from SonicWall found here: https://www.mysonicwall.com/

Additional recommendations and mitigation's for CVE-2024-40766 can be found in the respective link below:

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

UPDATE: SonicWall strongly advises that customers using GEN5 and GEN6 firewalls with SSLVPN users who have locally managed accounts immediately update their passwords to enhance security and prevent unauthorized access. Users can change their passwords if the "User must change password" option is enabled on their account. Administrators must manually enable the "User must change password" option for each local account to ensure this critical security measure is enforced.

Additionally, SonicWall recommends enabling MFA (TOTP or Email-based OTP) for all SSLVPN users. Resource: https://www.sonicwall.com/support/knowledge-base/how-do-i-configure-2fa-for-ssl-vpn-with-totp/190829123329169

[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 A068,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre