An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC 2501090162

NCSC Advisory

Multiple Vulnerabilities in SonicOS

9th, January 2025

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.

Description

CVE ID and CVSS Score[1]:

- CVE-2024-40762 (CVSS: 7.1)
- CVE-2024-53704 (CVSS: 8.2)
- CVE-2024-53705 (CVSS: 6.5)
- CVE-2024-53706 (CVSS: 7.8)

Published: 2025-01-09

Vendor: SonicWall

Product: SonicOS

Products Affected

CVE	Product	Version
CVE-2024-40762	• Gen7 Firewalls • Gen7 NSv • TZ80	• Gen7 Firewalls and NSv: Versions 7.1.x (7.1.1-7058 and older versions), and version 7.1.2-7019. • TZ80: Version 8.0.0-8035
CVE-2024-53704	• Gen7 Firewalls • Gen7 NSv • TZ80	• Gen7 Firewalls and NSv: Versions 7.1.x (7.1.1-7058 and older versions), and version 7.1.2-7019. • TZ80: Version 8.0.0-8035
CVE-2024-53705	• Gen6 Hardware Firewalls • Gen7 Firewalls • Gen7 NSv • TZ80	• Gen6 Hardware Firewalls: 6.5.4.15-117n and older versions. • Gen7 Firewalls and NSv: 7.0.x (7.0.1-5161 and older versions), 7.1.x (7.1.1-7058 and older versions), and version 7.1.2-7019. • TZ80: Version 8.0.0-8035
CVE-2024-53706	• Gen7 Cloud platform NSv	• Versions 7.1.x (7.1.1-7058 and older versions), • Version 7.1.2-7019.

[1] https://www.first.org/cvss/v3.0/specification-document

Impact

1) **CVE-2024-40762: CWE-338 - SonicOS SSLVPN Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)**

   in the SonicOS SSLVPN authentication token generator that, in certain cases, can be predicted by an attacker potentially resulting in authentication bypass.

2) **CVE-2024-53704: CWE-287 - SonicOS SSLVPN Authentication Bypass Vulnerability**

   An Improper Authentication vulnerability in the SSLVPN authentication mechanism allows a remote attacker to bypass authentication.

3) **CVE-2024-53705: CWE-918 - SonicOS SSH Management Server-Side Request Forgery Vulnerability**

   A Server-Side Request Forgery vulnerability in the SonicOS SSH management interface allows a remote attacker to establish a TCP connection to an IP address on any port when the user is logged in to the firewall.

4) **CVE-2024-53706: CWE-269 - Gen7 SonicOS Cloud NSv SSH Config Function Local Privilege Escalation Vulnerability**

   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 potentially lead to code execution.

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from SonicWall.

- https://nvd.nist.gov/vuln/detail/CVE-2024-40762
- https://www.cve.org/CVERecord?id=CVE-2024-40762
- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0003