مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – SonicOS

Tracking #:432316714

Date:08-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that SonicWall has issued a critical security advisory addressing multiple vulnerabilities in its SonicOS operating system, impacting both Gen6 and Gen7 hardware firewalls.

TECHNICAL DETAILS:

SonicWall has issued a critical security advisory addressing multiple vulnerabilities in its SonicOS operating system, impacting both Gen6 and Gen7 hardware firewalls. The vulnerabilities include authentication bypasses, privilege escalation, and other security flaws that could potentially expose devices to cyberattacks. Four significant vulnerabilities have been identified, with CVSS scores ranging from 6.5 to 8.2, indicating moderate to high severity.

Key vulnerabilities include:

- CVE-2024-53704 (CVSS 8.2): Authentication bypass in SonicOS SSLVPN
- CVE-2024-40762 (CVSS 7.1): Weak pseudo-random number generator in SSLVPN authentication
- CVE-2024-53706 (CVSS 7.8): Privilege escalation in Gen7 SonicOS Cloud NSv
- CVE-2024-53705 (CVSS 6.5): Server-side request forgery in SSH management

Fixed Versions:

- Gen6 Hardware Firewalls: Update to version 6.5.5.1-6n or higher
- Gen7 Firewalls: Update to version 7.1.3-7015 or higher
- Gen7 NSv: Update to version 7.0.1-5165 or higher
- TZ80: Update to version 8.0.0-8037 or higher

RECOMMENDATIONS:

- SonicWall strongly advises that users update their systems immediately to the latest versions that address these vulnerabilities.
- Limit access to SSLVPN and SSH management interfaces to trusted IP addresses and trusted networks.
- Review logs and network traffic for any signs of exploitation, such as unusual access attempts or connections to internal systems from unknown external IP addresses.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0003