CERT-EU

Security Advisory 2024-089

Critical Vulnerability in SonicWall SonicOS

August 26, 2024 — v1.0

TLP:CLEAR

History:

- *26/08/2024 — v1.0 – Initial publication*

Summary

On August 23, 2024, SonicWall issued a security advisory regarding a critical access control vulnerability (**CVE-2024-40766**) in its SonicOS. This flaw could allow attackers to gain unauthorised access to resources or cause the firewall crash [1].

It is recommended updating as soon as possible.

Technical Details

The vulnerability `CVE-2024-40766`, with a CVSS score of 9.3, is caused by improper access control in the SonicOS management interface, potentially leading to unauthorised access and firewall crashes [2].

Affected Products

- Gen 5: SOHO devices running version 5.9.2.14-12o and older;
- Gen 6: TZ, NSA, and SM models running versions 6.5.4.14-109n and older;
- Gen 7: TZ and NSA models running SonicOS build version 7.0.1-5035 and older.

Recommendations

CERT-EU recommends updating to the latest firmware versions immediately. It is also strongly advised restricting the firewall management access only to trusted sources, or disable WAN management access from the internet.

References

[1] https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-critical-access-control-flaw-in-sonicos/

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