CERT-EU

Security Advisory 2025-029

Possible Zero-Day Vulnerability in SonicWall Products

2025-08-05 — v1.0

TLP:CLEAR

History:

- *05/08/2025 — v1.0 – Initial publication*

Summary

On August 4, 2025, SonicWall issued an advisory regarding a possible zero-day vulnerability in the Gen 7 SonicWall firewalls [1]. A remote attacker could exploit this vulnerability to execute arbitrary code on the affected appliance. This vulnerability is being exploited in the wild [2].

It is recommended to disable SSLVPN Services as soon as possible.

Products Affected

The vulnerability seems to be affecting Gen 7 SonicWall firewalls. The vendor is investigating, but at the time of this writing, no more details are available [1].

Recommendations

It is strongly recommended to follow the vendor guidance [1]:

- Enable Security Services
- Enforce Multi-Factor Authentication (MFA)
- Remove Unused Accounts
- Practice Good Password Hygiene

Mitigation

Following the vendor guidance [1] should help prevent exploitation:

- Disable SSLVPN Services Where Practical
- Limit SSLVPN connectivity to trusted source IPs.

References

[1] https://www.sonicwall.com/support/notices/gen-7-sonicwall-firewalls-sslvpn-recent-threat-activity/250804095336430

[2] https://www.huntress.com/blog/exploitation-of-sonicwall-vpn