August 26, 2024

Overall Rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of SonicWall published a security advisory to address a critical vulnerability in the following products:

- SonicWall SOHO (Gen 5) – versions prior to 5.9.2.14-13o
- SonicWall SOHO (Gen 6) – versions prior to 6.5.2.8-2n (SM9800, NSsp 12400, NSsp 12800) and 6.5.4.15.116n (other Gen6 Firewall appliances)
- SonicWall SOHO (Gen 7) – versions 7.0.1-5035 and prior

Technical Details

An improper access control vulnerability has been identified in the SonicWall SonicOS management access, potentially leading to unauthorized 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 rated as a **CRITICAL** risk. Software updates exist to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at vulnerabilityandriskmanagement@gov.bc.ca

References

- CVE-2024-40766
- SonicWall Security Advisory – SNWLID-2024-0015
- SonicWall Security Advisories