January 17, 2024

Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

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

- SonicWall Capture Client – version 3.7.10 and prior.
- NetExtender Windows Client – version 10.2.337 and prior.

Exploitation of this vulnerability could result in a denial of service or execution of arbitrary code.

Technical Details

SonicWall Capture Client version 3.7.10 and NetExtender Client Windows client 10.2.337 and earlier versions are being installed with sfpmonitor.sys driver. The client applications communicate with the driver through queries. The driver method that handles those queries has Stack-based Buffer Overflow vulnerability that allows an attacker to craft a specific query to overwrite kernel memory, causing Denial of Service (DoS) which potentially leads to code execution in the target operating system.
SonicWall strongly advises Capture Client and SSL VPN NetExtender client users to upgrade to the latest release version.

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-6340
- GSonicWall Security Advisory – SNWLID-2023-6340
- SonicWall Security Advisories