July 22, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Sonicwall published security advisories to address vulnerabilities in multiple products. Included were updates for the following products:

- SonicOS IPSEC VPN – multiple products and versions
- SMA100 NetExtender Windows Client – versions 10.2.339 and prior

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.

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

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-2024-40764 CVE-2023-6340 CVE-2024-29014 CVE-2024-6387
- Sonicwall security advisories