Security Advisory
Vulnerability List
Report Vulnerability
Vulnerability Policy
Hall of Fame
RSS Feed

Security Advisory

Vulnerability List

/ Security Advisory / Vulnerability List

SFPMONITOR.SYS KOOB WRITE VULNERABILITY
8.2

OVERVIEW

Advisory ID	SNWLID-2023-6340
First Published	2024-01-17
Last Updated	2024-01-17
Workaround	false
Status	Applicable
CVE	CVE-2023-6340
CWE	CWE-121
CVSS v3	8.2
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H
Direct Link	

SUMMARY

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.

AFFECTED PRODUCT(S)

Capture Client 3.7.10 and earlier versions.

NetExtender Windows Client 10.2.337 (Windows 32 and 64 bit) and earlier versions.

CPE(S)

WORKAROUND

None

FIXED SOFTWARE

Capture Client 3.7.11 and higher versions.

NetExtender Windows Client 10.2.338 (Windows 32 and 64 bit) and higher versions.

COMMENTS

CREDIT(S)

Vladimir Tokarev of Section 52, Microsoft CPS Team

REVISION HISTORY

Version	Date	Description
1.0	16-Jan-2024	Initial Release.

REFERENCE(S)