Advisory Alert

Alert Number: AAA20220829 **Date:** August 29, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SonicWALL	**High**	Heap-based Buffer Overflow vulnerability

Description

Affected Product	**SonicWALL**
Severity	**High**
Affected Vulnerability	Heap-based Buffer Overflow vulnerability (CVE-2022-2915)
Description	SonicWALL has released a security update addressing a Heap-based Buffer Overflow vulnerability that exists in the SonicWALL SMA100 appliance. This vulnerability allows a remote authenticated attacker to cause Denial of Service (DoS) on the appliance or potentially lead to code execution. SonicWALL highly recommends to apply necessary fixes at earliest to avoid issues
Affected Products	SMA100 firmware 10.2.1.5-34sv and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0019

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.