Advisory Alert

Alert Number : **AAA20220314** **Date :** **March 14, 2022**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SonicWall	**High**	**Post Authentication OS Command Injection**

Description

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Post Authentication OS Command Injection(CVE-2022-22273)
Description	Sonicwall has released security updates addressing Post Authentication OS Command Injection vulnerability that exists in their products. The threat actors actively targeting end-of-life Secure Remote Access (SRA) series products, specifically appliances running all 8.x or 9.0.0.5-19sv and earlier versions. And Secure Mobile Access (SMA) 100 series products running old firmware 9.0.0.9-26sv and earlier versions. Sonicwall highly recommends to apply necessary fixes immediately to avoid issues.
Affected Products	SRA Series 9.0.0.5-19sv and earlier versions. SMA100 Series 9.0.0.9-26sv and earlier versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0001

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.