Advisory Alert

Alert Number : AAA20210111 **Date :** January 11, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SONICWALL	**High**	Multiple Vulnerabilities

Description

Affected Product	SONICWALL
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Sonicwall has released security patch updates addressing multiple vulnerabilities that exists in their products. CVE-2020-5147 – A local attacker could gain elevated privileges in the host operating system using an unquoted service path vulnerability that exists in SonicWall NetExtender Windows clients. CVE-2020-5146 - An authenticated management-user could perform OS command injection using HTTP POST parameters due to a flaw that exists in the SonicWall SMA100 appliance.
Affected Products	SMA100 build version 10.2.0.2-20sv and earlier. SonicWall NetExtender Windows client version 10.2.300 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0023 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0022

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.