



Advisory Alert

Alert Number : AAA20220328 Date : March 28, 2022

Document Classification Level : **Public Circulation Permitted | Public**

Information Classification Level : **TLP: WHITE**

Overview

Product	Severity	Vulnerability
SonicWall	Critical	Buffer overflow vulnerability

Description

Affected Product	SonicWall
Severity	Critical
Affected Vulnerability	Buffer overflow vulnerability (CVE-2022-22274)
Description	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service or potentially results in code execution in the firewall.
Affected Products	SonicWall appliances 7.0.1-5050 and older SonicWall appliances 7.0.1-R579 and older SonicWall appliances 6.5.4.4-44v-21-1452 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003

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.