Advisory Alert

Alert Number : AAA20210316 **Date :** March 16, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Sonicwall	**High**	Multiple Vulnerabilities
cPanel	**High**	Bypass implemented security restrictions

Description

Affected Product	**Sonicwall**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-20017, CVE-2021-20018)
Description	Sonicwall released security patches addressing multiple vulnerabilities that exists in the product. CVE-2021-20017: A post authenticated command injection vulnerability in SonicWall SMA100 allows an authenticated attacker to execute OS commands as a nobody user. CVE-2021-20018: A post-authenticated vulnerability in SonicWall SMA100 allows an attacker to export the configuration file to the specified email address.
Affected Products	SMA100 version 10.2.0.5 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0004 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0005

Affected Product	**cPanel**
Severity	**High**
Affected Vulnerability	Bypass implemented security restrictions
Description	cPanel has released security updates addressing unspecified error that exists in cPanel and WHM versions. Using this vulnerability attacker can bypass implemented security restrictions and perform unauthorized actions.
Affected Products	94.0.3 and Greater 92.0.12 and Greater 86.0.38 and Greater
Officially Acknowledged by the Vendor	yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/cpanel-tsr-2021-0002-announcement/

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.