Advisory Alert

Alert Number: **AAA20240226** **Date:** **February 26, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Multiple Vulnerabilities
F5	**High**	Use-after-free Vulnerabilities
cPanel	**High**, **Medium**	Multiple Vulnerabilities
SonicWall	**Medium**	Improper Access Control Vulnerability

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235)
Description	Dell has issued a security update for the PowerEdge T30 and T40 Mini Tower Server models, addressing multiple vulnerabilities in the Tianocore EDK2 third party component. These vulnerabilities could potentially be exploited by malicious users to compromise the affected systems. Dell recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	PowerEdge T30 BIOS Versions prior to 1.14.0 PowerEdge T40 BIOS Versions prior to 1.15.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000222073/dsa-2024-080-security-update-for-dell-poweredge-t30-t40-mini-tower-server-for-tianocore-edk2-vulnerabilities

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Use-after-free Vulnerabilities (CVE-2023-4206, CVE-2023-4207, CVE-2023-4208)
Description	F5 has released security updates addressing Use-after-free vulnerabilities that exist in their product. A local user could exploit these vulnerabilities to crash the system or potentially escalate their privileges on the system. F5 recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	Traffix SDC Version 5.2.0 CF1-5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000138693

Affected Product	**cPanel**
Severity	**High , Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21892, CVE-2024-22019, CVE-2024-21896, CVE-2024-22017, CVE-2023-46809, CVE-2024-21891, CVE-2024-21890, CVE-2024-22025)
Description	CPanel has released security updates addressing multiple vulnerabilities that exist in their cPanel EasyApache. It is highly recommended to apply necessary fixes provided on the official cPanel website at the earliest to avoid these security issues and all cPanel users are encouraged to upgrade latest versions
Affected Products	All versions of NodeJS 20 through 20.11.0. All versions of NodeJS 18 through 18.19.0.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-2024-02-21-maintenance-and-security-release/

Affected Product	**SonicWall**
Severity	**Medium**
Affected Vulnerability	Improper Access Control Vulnerability (CVE-2024-22395)
Description	SonicWall has released security updates addressing an Improper Access Control Vulnerability that exist in their products. This vulnerability could allow a remote authenticated attacker to associate another user's MFA mobile application, potentially compromising the security of the affected system. SonicWall strongly advises all users of SMA 100 series products to upgrade to the fixed release version 10.2.1.11-65sv or higher to address this vulnerability
Affected Products	Impacted Products - SMA 100 Series (SMA 200, 210, 400, 410, 500v) Impacted Versions - 10.2.1.10-62sv and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0001

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.