Advisory Alert

Alert Number: AAA20240409 **Date:** April 9, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Use-After-Free Vulnerability
cPanel	**High**, **Medium**, **Low**	Multiple Vulnerabilities
OpenSSL	**Low**	Denial of Service Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products that in turn affect Dell products. Exploitation of these vulnerabilities could lead to Local privilege escalation, Heap based buffer overflow, Integrity checks bypass, Cookie smuggling. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Storage Resource Manager (vApp) Versions prior to 4.10.0.3 Dell Storage Monitoring and Reporting (vApp) Versions prior to 4.10.0.3 Dell Storage Resource Manager (Windows/Linux Update) Versions prior to 4.10.0.3 Dell Storage Monitoring and Reporting (Windows Update/Linux Update) Versions prior to 4.10.0.3 Dell NetWorker (NetWorker Server) Version 19.10, Versions 19.8.0.4 and Prior.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000223919/dsa-2024-017-dell-storage-resource-manager-srm-and-dell-storage-monitoring-and-reporting-smr-security-update-for-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000223914/dsa-2024-166-security-update-for-dell-networker-curl-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Use-After-Free Vulnerability (CVE-2023-51779)
Description	SUSE has released security updates addressing a Use-After-Free Vulnerability that exists in their products. The vulnerability is caused due to a bt_sock_ioctl race condition in bt_sock_recvmsg in the Linux kernel. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20241153-1/

Affected Product	**cPanel**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-24795, CVE-2024-27316, CVE-2023-38709, CVE-2024-27983, CVE-2024-27982, CVE-2024-28182)
Description	cPanel has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, HTTP Request Smuggling and Excessive CPU usage. cPanel recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	cPanel All versions of ea-apache24 through 2.4.58 cPanel All versions of ea-nodejs18 through 18.20.0 cPanel All versions of ea-nodejs20 through 20.12.0 cPanel All versions of ea-nghttp2 through 1.60.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-2024-04-08-maintenance-and-security-release/

Affected Product	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2024-2511)
Description	OpenSSL has released security updates addressing a Denial of Service vulnerability cause due to unbounded memory growth when processing TLSv1.3 sessions. OpenSSL recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSSL 3.2, 3.1, 3.0, 1.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20240408.txt

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.