Advisory Alert

Alert Number: AAA20250324 **Date:** March 24, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
cPanel	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47633, CVE-2022-1048, CVE-2022-3303, CVE-2022-49272, CVE-2022-49288, CVE-2022-49291, CVE-2022-49545, CVE-2022-49733, CVE-2024-56658, CVE-2024-57996, CVE-2025-21718, CVE-2025-21772)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their SUSE Linux Enterprise products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise Server 11 SP4 SUSE Linux Enterprise Server 11 SP4 LTSS EXTREME CORE
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-20250983-1/

Affected Product	**cPanel**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-1736, CVE-2025-1861, CVE-2025-1734, CVE-2025-1217, CVE-2025-1219, CVE-2024-11235)
Description	cPanel, L.L.C. has released security updates addressing multiple vulnerabilities in various PHP versions within EasyApache 4. These vulnerabilities could be exploited by malicious users to compromise the affected system. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All versions of PHP 8.1 through 8.1.31. All versions of PHP 8.2 through 8.2.27. All versions of PHP 8.3 through 8.3.17. All versions of PHP 8.4 through 8.4.4.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-10-maintenance-and-security-release/

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.