Advisory Alert

Alert Number: AAA20230815 **Date:** August 15, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Suse	**High**	Linux Kernel Security updates
Dell	**High**	Multiple Vulnerabilities
Cpanel	**Medium**	Security Update

Description

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-40982, CVE-2023-0459, CVE-2023-20569 CVE-2023-21400, CVE-2023-2156, CVE-2023-2166, CVE-2023-31083, CVE-2023-3268, CVE-2023-3567, CVE-2023-3609, CVE-2023-3611, CVE-2023-3776, CVE-2023-38409, CVE-2023-3863, CVE-2023-4004, CVE-2023-3776, CVE-2023-1829, CVE-2023-20593, CVE-2023-2430, CVE-2023-2985, CVE-2023-3090, CVE-2023-3111, CVE-2023-3117, CVE-2023-31248, CVE-2023-3212, CVE-2023-3389, CVE-2023-3390, CVE-2023-35001, CVE-2023-3812)
Description	Suse has released security updates addressing Linux Kernel Security updates affecting their products. Exploitation of these vulnerabilities could lead multiple security flows. Suse recommends to apply the necessary security fixes at your earliest to avoid issues
Affected Products	Basesystem Module 15-SP5 Development Tools Module 15-SP5 Legacy Module 15-SP5 openSUSE Leap 15.5 SUSE Linux Enterprise Desktop 15 SP5 SUSE Linux Enterprise High Availability Extension 15 SP5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Workstation Extension 15 SP5 Basesystem Module 15-SP4 Development Tools Module 15-SP4 Legacy Module 15-SP4 openSUSE Leap 15.4 openSUSE Leap Micro 5.3 openSUSE Leap Micro 5.4 SUSE Linux Enterprise Desktop 15 SP4 SUSE Linux Enterprise High Availability Extension 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro for Rancher 5.3 SUSE Linux Enterprise Micro for Rancher 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Workstation Extension 15 SP4 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3 SUSE Linux Enterprise High Availability Extension 12 SP5 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 SUSE Linux Enterprise Software Development Kit 12 SP5 SUSE Linux Enterprise Workstation Extension 12 12-SP5 SUSE Real Time Module 15-SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20233311-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233313-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233309-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233302-1/

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-40982, CVE-2022-44611, CVE-2022-43505, CVE-2022-40982, CVE-2022-43505, CVE-2022-43505, CVE-2022-40982, CVE-2023-23908, CVE-2022-41804, CVE-2022-40982, CVE-2022-43505, CVE-2022-38083, CVE-2022-43505)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their PowerEdge products. That could be exploited by malicious users to compromise the affected systems Dell highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Multiple PowerEdge BIOS Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000216580/dsa-2023-206-security-update-for-dell-poweredge-server-for-intel-august-2023-security-advisories-2023-3-ipu

Affected Product	**cPanel**
Severity	**Medium**
Affected Vulnerability	Security Update
Description	cPanel has released updates addressing security fixes that exist in EasyApache 4 with libcurl. 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	EasyApache4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-2023-06-14-maintenance-and-security-release/

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.