Advisory Alert

Alert Number: **AAA20230824** **Date:** **August 24, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
CPanel	**Critical**	Buffer Overflow Vulnerability
Suse	**High**	Multiple Vulnerabilities
CPanel	**High**	XML External Entity Injection Vulnerability
Cisco	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	**CPanel**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2023-3824)
Description	CPanel has released security updates addressing a Buffer Overflow vulnerability that exists in third party components that in turn affect CPanel products. The vulnerability exist in PHP version 8.0.* before 8.0.30, 8.1.* before 8.1.22, and 8.2.* before 8.2.8, due to a boundary error within the phar_dir_read () function. A remote attacker can force the application to open a specially crafted .phar archive, trigger memory corruption and execute arbitrary code on the target system. CPanel highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	EasyApache4 All versions of PHP through 8.2.8.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-2023-08-23-maintenance-and-security-release/

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-40982, CVE-2023-0459, CVE-2023-20569, CVE-2023-20593, CVE-2023-2985, CVE-2023-34319, CVE-2023-35001, CVE-2023-3567, CVE-2023-3609, CVE-2023-3611, CVE-2023-3776, CVE-2023-4133, CVE-2023-4194, CVE-2023-3117, CVE-2023-3390, CVE-2023-3812, CVE-2023-2156, CVE-2023-31248, CVE-2023-3812)
Description	Suse has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of the vulnerabilities could lead to buffer overrun, out-of-bounds memory access, Information leakage, side channel attack. Suse recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	openSUSE Leap 15.4, 15.5 SUSE CaaS Platform 4.0 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise High Availability Extension 15 SP1, 15 SP2, 15 SP3 SUSE Linux Enterprise High Performance Computing 15 SP1 SUSE Linux Enterprise High Performance Computing 15 SP1 LTSS 15-SP1 SUSE Linux Enterprise High Performance Computing 15 SP2 SUSE Linux Enterprise High Performance Computing 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise High Performance Computing 15 SP3 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP3 SUSE Linux Enterprise High Performance Computing LTSS 15 SP3 SUSE Linux Enterprise Live Patching 15-SP1, 15-SP2, 15-SP3 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Server 15 SP1 SUSE Linux Enterprise Server 15 SP1 Business Critical Linux 15-SP1 SUSE Linux Enterprise Server 15 SP1 LTSS 15-SP1 SUSE Linux Enterprise Server 15 SP2 SUSE Linux Enterprise Server 15 SP2 Business Critical Linux 15-SP2 SUSE Linux Enterprise Server 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server 15 SP3 Business Critical Linux 15-SP3 SUSE Linux Enterprise Server 15 SP3 LTSS 15-SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP1, 15 SP2, 15 SP3 SUSE Manager Proxy 4.0, 4.1, 4.2 SUSE Manager Retail Branch Server 4.0, 4.1, 4.2 SUSE Manager Server 4.0, 4.1, 4.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20233392-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233390-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233391-1

Affected Product	**CPanel**
Severity	**High**
Affected Vulnerability	XML External Entity Injection Vulnerability (CVE-2023-3823)
Description	CPanel has released security updates addressing a XML Loading vulnerability that exists in third party components that in turn affect CPanel products. The vulnerability exist in PHP versions 8.0.* before 8.0.30, 8.1.* before 8.1.22, and 8.2.* before 8.2.8, due to insufficient validation of user-supplied XML input. A remote attacker can pass a specially crafted XML code to the affected application and view contents of arbitrary files on the system or initiate requests to external systems. CPanel recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	EasyApache4 All versions of PHP through 8.2.8.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-2023-08-23-maintenance-and-security-release/

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20168, CVE-2023-20169, CVE-2023-20200, CVE-2023-20115, CVE-2023-20234, CVE-2023-20230)
Description	Cisco has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities could lead to Denial Of Service and File read/overwrite. Cisco recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco products running a vulnerable release of Cisco NX-OS Software with the directed request option enabled for TACACS+, RADIUS, or both • MDS 9000 Series Multilayer Switches (CSCwe72670) • Nexus 1000 Virtual Edge for VMware vSphere (CSCwe72673) • Nexus 1000V Switch for Microsoft Hyper-V (CSCwe72673) • Nexus 1000V Switch for VMware vSphere (CSCwe72673) • Nexus 3000 Series Switches (CSCwe72648) • Nexus 5500 Platform Switches (CSCwe72674) • Nexus 5600 Platform Switches (CSCwe72674) • Nexus 6000 Series Switches (CSCwe72674) • Nexus 7000 Series Switches (CSCwe72368) • Nexus 9000 Series Switches in standalone NX-OS mode (CSCwe72648) Cisco products running Cisco NX-OS Software Release 10.3(2) and the IS-IS protocol enabled • Nexus 3000 Series Switches • Nexus 9000 Series Switches in standalone NX-OS mode Cisco products running a vulnerable release of Cisco FXOS Software or Cisco UCS Software and have the SNMP service enabled • Firepower 4100 Series (CSCvi80806) • Firepower 9300 Security Appliances (CSCvi80806) • UCS 6300 Series Fabric Interconnects (CSCwd38796, CSCwe12029) Cisco products running a vulnerable release of Cisco NX-OS Software and had the SFTP server feature enabled • Nexus 3000 Series Switches • Nexus 9000 Series Switches in standalone NX-OS mode Cisco products running a vulnerable release of Cisco FXOS Software: • Firepower 1000 Series (CSCwd35726, CSCwd05772) • Firepower 2100 Series (CSCwd35726, CSCwd05772) • Firepower 4100 Series (CSCwb91812, CSCwd35722) • Firepower 9300 Security Appliances (CSCwb91812, CSCwd35722) • Secure Firewall 3100 Series (CSCwd35726, CSCwd05772) Cisco APIC when restricted security domains were configured.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-remoteauth-dos-XB6pv74m https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-n3_9k-isis-dos-FTCXB4Vb https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fp-ucsfi-snmp-dos-qtv69NAO https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-sftp-xVAp5Hfd https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxos-arbitrary-file-BLk6YupL https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-uapa-F4TAShk

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.