Advisory Alert

Alert Number: AAA20231013 **Date:** October 13, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Multiple Vulnerabilities
cPanel	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-32081, CVE-2022-32082, CVE-2022-32084, CVE-2022-32089, CVE-2022-32091, CVE-2022-38791, CVE-2022-47015, CVE-2023-5157, CVE-2023-3341, CVE-2018-14041, CVE-2018-20676, CVE-2018-20677, CVE-2023-43040)
Description	Red Hat has released several important security updates to address vulnerabilities in various products. It is strongly recommended to apply these updates to your systems to ensure the security and integrity of your Red Hat environment.
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.0 s390x Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux Workstation 7 x86_64 Red Hat Enterprise Linux Desktop 7 x86_64 Red Hat Enterprise Linux for IBM z Systems 7 s390x Red Hat Enterprise Linux for Power, big endian 7 ppc64 Red Hat Enterprise Linux for Scientific Computing 7 x86_64 Red Hat Enterprise Linux for Power, little endian 7 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:5683 https://access.redhat.com/errata/RHSA-2023:5684 https://access.redhat.com/errata/RHSA-2023:5689 https://access.redhat.com/errata/RHSA-2023:5690 https://access.redhat.com/errata/RHSA-2023:5691 https://access.redhat.com/errata/RHSA-2023:5693

Affected Product	**cPanel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-44487, CVE-2023-38545, CVE-2023-38546, CVE-2023-45648, CVE-2023-42795, CVE-2023-42794)
Description	cPanel has released Security Updates addressing multiple vulnerabilities that exist in their products.If exploited these vulnerabilities can leads to denial of service (DoS) attack, heap-based buffer overflow, execute arbitrary code, HTTP request to the server, smuggle arbitrary HTTP headers, information leaking. cPanel Tomcat recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	All versions of libcurl from 7.9.1 (CVE-2023-38546) and 7.69.0 (CVE-2023-38545) through 8.3.0. All versions of ea-tomcat from 8.5.0 through 8.5.93. All versions of ea-nghttp2 through 1.56.0.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-2023-10-12-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.