Advisory Alert

Alert Number: **AAA20241126** **Date:** **November 26, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
cPanel	**Critical**	Out-Of-Bounds Write Vulnerability
cPanel	**Medium**	Multiple Vulnerabilities
Palo Alto	**Medium**	Privilege Escalation Vulnerability
F5	**Medium**	Multiple Vulnerabilities
Red Hat	**Medium, Low**	Multiple Vulnerabilities

Description

Affected Product	**cPanel**
Severity	**Critical**
Affected Vulnerability	Out-Of-Bounds Write Vulnerability (CVE-2024-8932)
Description	cPanel has released security updates addressing an Out-Of-Bounds Write Vulnerability that exists in their products. **CVE-2024-8932** - In PHP versions 8.1.* before 8.1.31, 8.2.* before 8.2.26, 8.3.* before 8.3.14, uncontrolled long string inputs to ldap_escape() function on 32-bit systems can cause an integer overflow. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EasyApache4 All versions of PHP 8.1 through 8.1.30 EasyApache4 All versions of PHP 8.2 through 8.2.25 EasyApache4 All versions of PHP 8.3 through 8.3.13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-2024-11-25-maintenance-and-security-release/

Affected Product	**cPanel**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-11233, CVE-2024-11234, CVE-2024-11236, CVE-2024-8929)
Description	CPanel has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-11233** - In PHP versions 8.1.* before 8.1.31, 8.2.* before 8.2.26, 8.3.* before 8.3.14, due to an error in convert.quoted-printable-decode filter certain data can lead to buffer overread by one byte, which can in certain circumstances lead to crashes or disclose content of other memory areas. **CVE-2024-11234** - In PHP versions 8.1.* before 8.1.31, 8.2.* before 8.2.26, 8.3.* before 8.3.14, when using streams with configured proxy and "request_fulluri" option, the URI is not properly sanitized which can lead to HTTP request smuggling and allow the attacker to use the proxy to perform arbitrary HTTP requests originating from the server, thus potentially gaining access to resources not normally available to the external user. **CVE-2024-11236** - In PHP versions 8.1.* before 8.1.31, 8.2.* before 8.2.26, 8.3.* before 8.3.14, uncontrolled long string inputs to ldap_escape() function on 32-bit systems can cause an integer overflow, resulting in an out-of-bounds write. **CVE-2024-8929** - In PHP versions 8.1.* before 8.1.31, 8.2.* before 8.2.26, 8.3.* before 8.3.14, a hostile MySQL server can cause the client to disclose the content of its heap containing data from other SQL requests and possible other data belonging to different users of the same server. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EasyApache4 All versions of PHP 8.1 through 8.1.30 EasyApache4 All versions of PHP 8.2 through 8.2.25 EasyApache4 All versions of PHP 8.3 through 8.3.13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-2024-11-25-maintenance-and-security-release/

Affected Product	**Palo Alto**
Severity	**Medium**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2024-5921)
Description	Palo Alto has released security updates addressing a Privilege Escalation Vulnerability that exists in their products. **CVE-2024-5921** - An insufficient certification validation issue in the Palo Alto Networks GlobalProtect app enables attackers to connect the GlobalProtect app to arbitrary servers. This can enable an attacker to install malicious root certificates on the endpoint and subsequently install malicious software signed by the malicious root certificates on that endpoint. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	GlobalProtect App 6.3 all versions GlobalProtect App 6.2 versions less than 6.2.6 on Windows GlobalProtect App 6.2 all versions on MacOS and Linux GlobalProtect App 6.1 all versions GlobalProtect App 6.0 all versions GlobalProtect App 5.1 all versions GlobalProtect UWP App all versions on Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2024-5921

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-3858, CVE-2019-3862)
Description	F5 has issued security updates addressing multiple vulnerabilities that exist in their products. **CVE-2019-3858** - An out of bounds read flaw was discovered in libssh2 before 1.8.1 when a specially crafted SFTP packet is received from the server. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. **CVE-2019-3862** - An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit status message and no payload are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IQ Centralized Management 8.2.0 - 8.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000148713

Affected Product	**Red Hat**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-4204,CVE-2021-47393,CVE-2021-47461,CVE-2022-0500,CVE-2022-23222,CVE-2022-48686,CVE-2022-48773,CVE-2022-48929,CVE-2023-0597,CVE-2023-52489,CVE-2024-26671,CVE-2024-26961,CVE-2024-31076,CVE-2024-35823,CVE-2024-36889,CVE-2024-36920,CVE-2024-38564,CVE-2024-40988,CVE-2024-41009,CVE-2024-41014,CVE-2024-41023,CVE-2024-46858,CVE-2022-48786,CVE-2024-42244,CVE-2024-50226,CVE-2024-27043,CVE-2024-27399)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause privilege escalation, information leakage, race conditions, system crash. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8 s390x 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 - 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 CodeReady Linux Builder for x86_64 - Extended Update Support 8.8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.8 aarch64 Red Hat Enterprise Linux Server - AUS 8.4 x86_64 Red Hat Enterprise Linux Server - TUS 8.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Real Time 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV 9 x86_64 Red Hat Enterprise Linux for ARM 64 9 aarch64 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 Real Time - Telecommunications Update Service 8.4 x86_64 Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.4 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:10262 • https://access.redhat.com/errata/RHSA-2024:10265 • https://access.redhat.com/errata/RHSA-2024:10273 • https://access.redhat.com/errata/RHSA-2024:10274 • https://access.redhat.com/errata/RHSA-2024:10275 • https://access.redhat.com/errata/RHSA-2024:10281 • https://access.redhat.com/errata/RHSA-2024:10282

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.