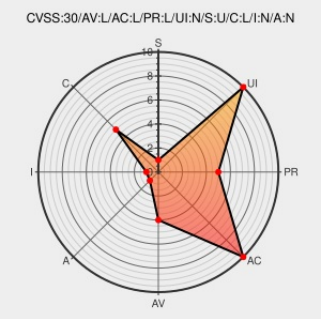
CVE-2017-18424

Published on: 08/02/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:55 PM UTC

CVE-2017-18424

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Cpanel from Cpanel contain the following vulnerability:

In cPanel before 66.0.2, the Apache HTTP Server configuration file is changed to world-readable when rebuilt (SEC-274).

CVE-2017-18424 has been assigned by cve@mitre.org to track the vulnerability - currently rated as LOW severity.

CVSS3 Score: 3.3 - LOW

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
66 Change Log - Change Logs - cPanel Documentation	Release Notes Vendor Advisory documentation.cpanel.net text/html	CONFIRM documentation.cpanel.net/display/CL/66+Change+Log

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cpanel	Cpanel	All	All	All	All
Application	Cpanel	Cpanel	All	All	All	All

cpe:2.3:a:cpanel:cpanel:*:*:*:*:*:*:*:*:

cpe:2.3:a:cpanel:cpanel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report