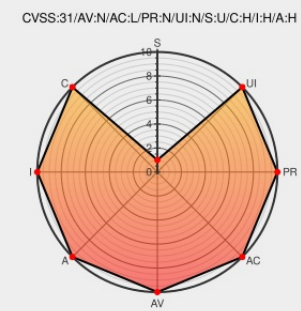
CVE-2021-20850

Published on: 11/24/2021 12:00:00 AM UTC

Last Modified on: 11/29/2021 05:16:00 PM UTC

CVE-2021-20850

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Powercms from Alfasado contain the following vulnerability:

PowerCMS XMLRPC API of PowerCMS 5.19 and earlier, PowerCMS 4.49 and earlier, PowerCMS 3.295 and earlier, and PowerCMS 2 Series (End-of-Life, EOL) allows a remote attacker to execute an arbitrary OS command via unspecified vectors.

CVE-2021-20850 has been assigned by vultures@jpcert.or.jp to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Alfasado Inc.** - **PowerCMS XMLRPC API** version **PowerCMS 5.19 and earlier, PowerCMS 4.49 and earlier, PowerCMS 3.295 and earlier, PowerCMS 2 Series (End-of-Life, EOL)**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
PowerCMS 5.19 / 4.49 / 3.295 向けパッチについて (XMLRPC API における OS コマンド・インジェクションの脆弱性対策) | 新着情報 | PowerCMS - カスタマ	www.powercms.jp text/html	MISC www.powercms.jp/news/release-

イズする CMS。	text/html	patch-xmlrpc-api-202110.html
JVN#17645965: PowerCMS XMLRPC API vulnerable to OS command injection	jvn.jp text/xml	MISC jvn.jp/en/jp/JVN17645965/index.html

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	Alfasado	Powercms	All	All	All	All
Application	Alfasado	Powercms	All	All	All	All
Application	Alfasado	Powercms	All	All	All	All
Application	Alfasado	Powercms	All	All	All	All

cpe:2.3:a:alfasado:powercms:*:*:*:*:*:*:*:*:

cpe:2.3:a:alfasado:powercms:*:*:*:*:*:*:*:*:

cpe:2.3:a:alfasado:powercms:*:*:*:*:*:*:*:*:

cpe:2.3:a:alfasado:powercms:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-20850 : PowerCMS XMLRPC API of PowerCMS 5.19 and earlier, PowerCMS 4.49 and earlier, PowerCMS 3.295 and ea… twitter.com/i/web/status/1…	2021-11-24 10:46:08
@usijoe	IT Risk: PowerCMS の XMLRPC API には、OS コマンドインジェクションの脆弱性が存在します 遠隔の第三者によって、任意の OS コマンドを実行される可能性があります。 CVE-2021-20850… twitter.com/i/web/status/1…	2021-11-24 11:04:12

← Previous ID

Next ID→

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