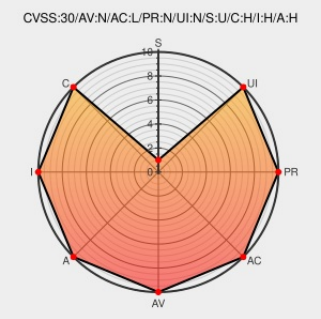
CVE-2018-16731

Published on: 09/08/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:33 PM UTC

CVE-2018-16731

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



Certain versions of Cscms from Chshcms contain the following vulnerability:

CScms 4.1 allows arbitrary file upload by (for example) adding the php extension to the default filetype list (gif, jpg, png), and then providing a .php pathname within fileurl JSON data.

CVE-2018-16731 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

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
CScms/CScms_up.md at master · AvaterXXX/CScms · GitHub	Third Party Advisory, github.com, text/html	MISC github.com/AvaterXXX/CScms/blob/master/CScms_up.md
error	Exploit	MISC www.patec.cn/newsshow.php?cid=24&id=123

Third Party Advisory
www.patec.cn
text/html
Inactive Link Not Archived

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	Chshcms	Cscms	4.1	All	All	All
Application	Chshcms	Cscms	4.1	All	All	All

cpe:2.3:a:chshcms:cscms:4.1:*:*:*:*:*:*:*:

cpe:2.3:a:chshcms:cscms:4.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→