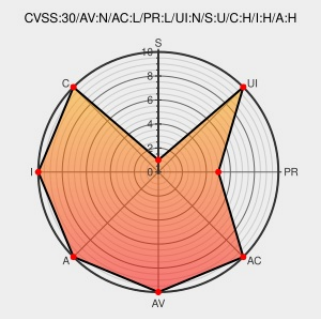
CVE-2018-19520

Published on: 11/25/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:40 PM UTC

CVE-2018-19520

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



Certain versions of Php from Php contain the following vulnerability:

An issue was discovered in SDCMS 1.6 with PHP 5.x. app/admin/controller/themecontroller.php uses a check_bad function in an attempt to block certain PHP functions such as eval, but does not prevent use of preg_replace 'e' calls, allowing users to execute arbitrary code by leveraging access to admin template management.

CVE-2018-19520 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
	Exploit Third Party Advisory blog.whiterabbitxyj.com application/msword	MISC blog.whiterabbitxyj.com/cve/SDCMS_1.6_code_

WhiteRabbitc.github.io/SDCMS_1.6_code_execution.doc at master · WhiteRabbitc/WhiteRabbitc.github.io · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/WhiteRabbitc/WhiteRabbitc.github.io/blob/ma

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	Php	Php	All	All	All	All
Application	Sdcms	Sdcms	1.6	All	All	All
Application	Sdcms	Sdcms	1.6	All	All	All

cpe:2.3:a:php:php:*:*:*:*:*:*:*:*:

cpe:2.3:a:sdcms:sdcms:1.6:*:*:*:*:*:*:*:

cpe:2.3:a:sdcms:sdcms:1.6:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→