

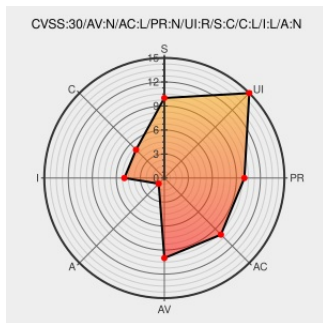


CVE-2018-18608

Published on: 10/23/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:52 PM UTC

CVE-2018-18608

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Dedecms](#) from [Dedecms](#) contain the following vulnerability:

DedeCMS 5.7 SP2 allows XSS via the function named GetPageList defined in the include/datalistcp.class.php file that is used to display the page numbers list at the bottom of some templates, as demonstrated by the PATH_INFO to /member/index.php, /member/pm.php, /member/content_list.php, or /plus/feedback.php.

CVE-2018-18608 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Reflected XSS Vulnerability exists in the	Exploit Third Party Advisory github.com	MISC github.com/ky-j/dedecms/issues/8

exists in the file of DedeCMS V5.7 SP2 · Issue #8 · ky-j/dedecms · GitHub

Exploit

Third Party Advisory

github.com

application/vnd.openxmlformats-officedocument.wordprocessingml.document

MISC github.com/ky-j/dedecms/files/2504649/Reflected.XSS.Vulnerability.ex

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	Dedecms	Dedecms	5.7	sp2	All	All
Application	Dedecms	Dedecms	5.7	sp2	All	All

cpe:2.3:a:dedecms:dedecms:5.7:sp2:*:*:*:*:*:

cpe:2.3:a:dedecms:dedecms:5.7:sp2:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →