

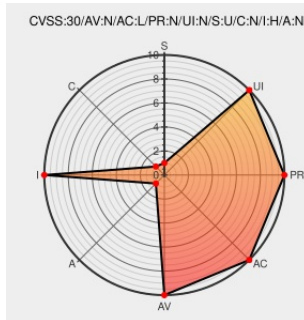


CVE-2019-8362

Published on: 02/16/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:55 PM UTC

CVE-2019-8362

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

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

DedeCMS through V5.7SP2 allows arbitrary file upload in dede/album_edit.php or dede/album_add.php, as demonstrated by a dede/album_edit.php?dopost=save&formzip=1 request with a ZIP archive that contains a file such as "1.jpg.php" (because input validation only checks that .jpg, .png, or .gif is present as a substring, and does not otherwise check the file name or content).

CVE-2019-8362 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
dedecms v5.7 sp2 文	Exploit Third Party Advisory	MISC tusk1.cn/2019/02/16/dedecms%20v5.7%20sp2%E6%96%87%E4%BB%B6%E4%B8%8A%E4%BC%A0

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	All	All	All	All
Application	Dedecms	Dedecms	5.7	-	All	All
Application	Dedecms	Dedecms	5.7	sp1	All	All
Application	Dedecms	Dedecms	5.7	sp2	All	All
Application	Dedecms	Dedecms	All	All	All	All
Application	Dedecms	Dedecms	5.7	-	All	All
Application	Dedecms	Dedecms	5.7	sp1	All	All
Application	Dedecms	Dedecms	5.7	sp2	All	All
cpe:2.3:a:dedecms:dedecms:*:*:*:*:*:						
cpe:2.3:a:dedecms:dedecms:5.7:-:*:*:*:*:						
cpe:2.3:a:dedecms:dedecms:5.7:sp1:*:*:*:*:						
cpe:2.3:a:dedecms:dedecms:5.7:sp2:*:*:*:*:						
cpe:2.3:a:dedecms:dedecms:*:*:*:*:*:						
cpe:2.3:a:dedecms:dedecms:5.7:-:*:*:*:*:						
cpe:2.3:a:dedecms:dedecms:5.7:sp1:*:*:*:*:						
cpe:2.3:a:dedecms:dedecms:5.7:sp2:*:*:*:*:						

No vendor comments have been submitted for this CVE

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)