

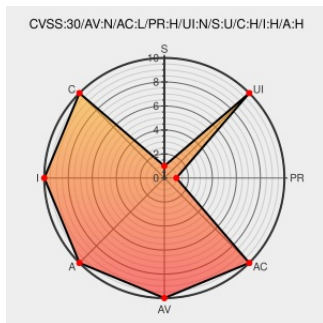


CVE-2015-9227

Published on: 09/11/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:21 PM UTC

CVE-2015-9227

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

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

PHP remote file inclusion vulnerability in the get_file function in upload/admin2/controller/report_logs.php in AlegroCart 1.2.8 allows remote administrators to execute arbitrary PHP code via a URL in the file_path parameter to upload/admin2.

CVE-2015-9227 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.2 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	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
AlegroCart 1.2.8 Local / Remote File Inclusion ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/134361/AlegroCart-1.2.8-Local-Remote-File-Inclusion.html

Full Disclosure: AlegroCart 1.2.8: LFI/RFI

Exploit

Mailing List

Third Party Advisory

seclists.org

text/html

FULLDISC 20151114 AlegroCart 1.2.8: LFI/RFI

Cureblog - Der Blog der Curesec GmbH

Exploit

Third Party Advisory

web.archive.org

text/html

Inactive Link

Not Archived

MISC blog.curesec.com/article/blog/AlegroCart-128-LFIRFI-102.html

AlegroCart 1.2.8 - Local/Remote File Inclusion - PHP webapps Exploit

Exploit

Third Party Advisory

VDB Entry

www.exploit-db.com

Proof of Concept

text/html

EXPLOIT-DB 38728

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	Alegrocart	Alegrocart	1.2.8	All	All	All
Application	Alegrocart	Alegrocart	1.2.8	All	All	All

cpe:2.3:a:alegrocart:alegrocart:1.2.8:*:*:*:*:*:

cpe:2.3:a:alegrocart:alegrocart:1.2.8:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→