



CVE-2015-7571

Published on: 08/07/2017 12:00:00 AM UTC

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

CVE-2015-7571

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

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

Unrestricted file upload vulnerability in Yeager CMS 1.2.1 allows remote attackers to execute arbitrary code by uploading a file with an executable extension.

CVE-2015-7571 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20160210 SEC Consult SA-20160210-0 :: Yeager CMS Multiple Vulnerabilities
Yeager CMS 1.2.1 - Multiple Vulnerabilities - PHP webapps Exploit	Exploit Third Party Advisory	EXPLOIT-DB 39436

VDB Entry
www.exploit-db.com
Proof of Concept
text/html

Full Disclosure: SEC Consult SA-20160210-0 ::
Yeager CMS Multiple Vulnerabilities

Exploit
Mailing List
Third Party Advisory
seclists.org
text/html

 FULLDISC 20160210 SEC Consult SA-20160210-0 ::
Yeager CMS Multiple Vulnerabilities

Yeager CMS 1.2.1 File Upload / SQL Injection /
XSS / SSRF ≈ Packet Storm

Exploit
Third Party Advisory
VDB Entry
packetstormsecurity.com
text/html

 MISC packetstormsecurity.com/files/135716/Yeager-CMS-1.2.1-File-Upload-SQL-Injection-XSS-SSRF.html

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	Yeager	Yeager Cms	1.2.1	All	All	All
Application	Yeager	Yeager Cms	1.2.1	All	All	All
cpe:2.3:a:yeager:yeager_cms:1.2.1:*:*:*:*:*:						
cpe:2.3:a:yeager:yeager_cms:1.2.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/cybersecurity	KashmirBlack botnet behind attacks on CMSs like WordPress, Joomla, Drupal, others (16 vulnerabilities exploited)	2020-10-26 09:38:41

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)