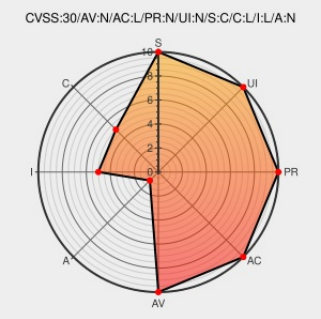
CVE-2015-7570

Published on: 04/24/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-7570

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



Certain versions of Yeager Cms from Yeager contain the following vulnerability:

Multiple server-side request forgery (SSRF) vulnerabilities in Yeager CMS 1.2.1 allow remote attackers to trigger outbound requests and enumerate open ports via the dbhost parameter to libs/org/adodb_lite/tests/test_adodb_lite.php, libs/org/adodb_lite/tests/test_datadictionary.php, or libs/org/adodb_lite/tests/test_adodb_lite_sessions.php.

CVE-2015-7570 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.2 - HIGH

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

CVSS2 Score: 6.4 - MEDIUM

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

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 Patch Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 39436
Full Disclosure: SEC Consult SA-20160210-0 :: Yeager CMS Multiple Vulnerabilities	Mailing List Patch 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 Patch Third Party Advisory packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/135716/Yeager-CMS-1.2.1-File-Upload-SQL-Injection-XSS-SSRF.html

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

← Previous ID

Next ID→