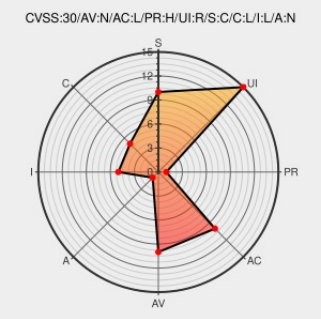
CVE-2018-11512

Published on: 05/28/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:17 PM UTC

CVE-2018-11512

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



Certain versions of Witycms from Creatiwity contain the following vulnerability:

Stored cross-site scripting (XSS) vulnerability in the "Website's name" field found in the "Settings" page under the "General" menu in Creatiwity wityCMS 0.6.1 allows remote attackers to inject arbitrary web script or HTML via a crafted website name by doing an authenticated POST HTTP request to admin/settings/general.

CVE-2018-11512 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.8 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
wityCMS 0.6.1 - Cross-Site Scripting - PHP webapps Exploit	Exploit Patch Third Party Advisory	EXPLOIT-DB 44790

	VDB Entry www.exploit-db.com Proof of Concept text/html	
Persistent XSS on 'Website's name' field (site_title) · Issue #150 · Creatiwity/witycms · GitHub	Exploit Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/Creatiwity/witycms/issues/150
#146 - Uses HTML purifier and htmlspecialchars in search app · Creatiwity/witycms@7967e5b · GitHub	Patch github.com text/html	MISC github.com/Creatiwity/witycms/commit/7967e5bf15b4d2ee6b85b56e82d7e1229147de

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	Creatiwity	Witycms	0.6.1	All	All	All
Application	Creatiwity	Witycms	0.6.1	All	All	All

cpe:2.3:a:creatiwity:witycms:0.6.1:*:*:*:*:*:*:*

cpe:2.3:a:creatiwity:witycms:0.6.1:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→