



CVE-2018-10026

Published on: 04/11/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:21 PM UTC

CVE-2018-10026

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

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

The WeChat module in YzmCMS 3.7.1 has reflected XSS via the admin/module/init.html echostr parameter, related to the valid function in application/wechat/controller/index.class.php.

CVE-2018-10026 has been assigned by [M](#) 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
Page not found · GitHub · GitHub	Exploit Third Party Advisory github.com text/html Inactive Link Not Archived	MISC github.com/SukaraLin/Drops/blob/master/YZMCMSxss.md

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yzmcms	Yzmcms	3.7.1	All	All	All
Application	Yzmcms	Yzmcms	3.7.1	All	All	All
cpe:2.3:a:yzmcms:yzmcms:3.7.1:*:*:*:*:*:						
cpe:2.3:a:yzmcms:yzmcms:3.7.1:*:*:*:*:*:						

← Previous ID

Next ID→

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.report and Source URL Uptime Status status.cve.report