



CVE-2021-40639

Published on: 09/15/2021 12:00:00 AM UTC

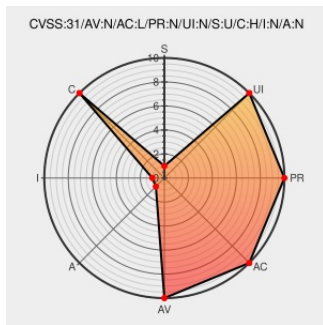
Last Modified on: 09/28/2021 03:33:00 PM UTC

CVE-2021-40639

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



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

Improper access control in Jfinal CMS 5.1.0 allows attackers to access sensitive information via `/classes/conf/db.properties&config=filemanager.config.js`.

CVE-2021-40639 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
GitHub - jflyfox/jfinal_cms: jfinal cms是一个java开发的功能强大的信息咨询网站，采用了简洁强大的JFinal作为web框架，模板引擎用的是beetl，数据库用mysql，前端bootstrap框架。支持oauth2认证、帐号注册、密码加密、评论及回复，消息提示，网站访问量统计，文章评论数和浏览量统计，回复管理，支持权限管理。后台模块包含：栏目管理，	github.com text/html	MISC github.com/jflyfox/jfinal_cms

栏目公告, 栏目滚动图片, 文章管理, 回复管理, 意见反馈, 我的相册, 相册管理, 图片管理, 专辑管理、视频管理、缓存更新, 友情链接, 访问统计, 联系人管理, 模板管理, 组织机构管理, 用户管理, 角色管理, 菜单管理, 数据字典管理。

File reading · Issue #27 · jflyfox/jfinal_cms · GitHub

[github.com](#)
[text/html](#)

 **MISC**
github.com/jflyfox/jfinal_cms/issues/27

No Description Provided

[jfinalcms.com](#)

[MISC jfinalcms.com](#)

Inactive Link Not Archived

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	Jflyfox	Jfinal Cms	5.1.0	All	All	All
<code>cpe:2.3:a:jflyfox:jfinal_cms:5.1.0:*:*:*:*:*::</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-40639 : Improper access control in Jfinal CMS 5.1.0 allows attackers to access sensitive information via /... twitter.com/i/web/status/1...	2021-09-15 22:07:48

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

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](#)