New issue

ZZCMS absolute path information disclosure vulnerability #1

⊙ **Open**   liong007 opened this issue on Sep 8 · 0 comments

---

liong007 commented on Sep 8 · edited ▾   Owner

[CVE-2022-40443](#)
Vulnerability Author：yuanlirong （袁利荣）
Attack vector(s):
zzcms is a set of content management system (CMS) of China's zzcms team.
Absolute path information disclosure vulnerability exists in zzcms 2022. An unauthenticated attacker can take advantage of this vulnerability by sending a get request to "/one/siteinfo.php" (the get request is changed to "//one/siteinfo.php") to obtain the error information returned by the server showing the location (absolute path) of the application.

Product:
ZZCMS

Version:
ZZCMS 2022

Vendor Homepage:
http://www.zzcms.net/

Software Link:
http://www.zzcms.net/download/zzcms2022.zip

or

https://github.com/liong007/ZZCMS/releases/download/ZZCMS2022/zzcms2022.zip

POC:
get request to "/one/siteinfo.php" changed to "//one/siteinfo.php", to obtain the error information returned by the server showing the location (absolute path) of the application.

Affected pages:
All pages that contain page /one/siteinfo.php

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant