New issue

Jump to bottom

Pluck 4.7.15 - Zip Slip Vulnerability #100

Closed naiagoesawoo opened this issue on Apr 21, 2021 · 2 comments

Labels Password Required for exploit Resolved Security:low

naiagoesawoo commented on Apr 21, 2021

Issue Summary
Pluck's module and theme installers are vulnerable to directory traversal (via zip slip).

Detailed Description
It is possible to upload a malicious zip file in order to traverse directories outside of the intended environment, potentially allowing arbitrary code execution which will run with the permissions of the user assigned to the webserver.

Reproduction Steps

1. Using the evilarc tool, create a zip archive containing a PHP file with a depth of 2 `(python evilarch.py shell.php -d 2 -f wolf.zip)`
2. Visit `<pluck_domain>/admin.php?action=themeinstall` and upload the malicious `wolf.zip` you created.
3. Visit `<pluck_domain>/shell.php` and you now have a PHP shell.

Impact
This vulnerability makes remote code execution under the privileges of the user running the webserver application possible.

BSteelooper added Password Required for exploit Security:low labels on Apr 21, 2021

BSteelooper added a commit that referenced this issue on Apr 26, 2021

`Fix for issue #100` `89c40c7`

BSteelooper commented on Apr 26, 2021 Contributor

Could you perform a retest with the latest dev version?

BSteelooper added the Resolved label on Apr 26, 2021

naiagoesawoo commented on Apr 26, 2021 Author

I confirm the Zip Slip vulnerability has been fixed.

naiagoesawoo closed this as completed on Apr 26, 2021

BSteelooper mentioned this issue on Dec 13, 2021

Pluck 4.7.15 - Zip Slip Vulnerability #105
Closed

Assignees
No one assigned

Labels
Password Required for exploit Resolved Security:low

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants