New issue

Jump to bottom

XSS vulnerability: CVS lastlog filename not escaped #211

Closed cmpilato opened this issue on Mar 26, 2020 · 2 comments

Labels bug

Milestone 1.2.1

cmpilato commented on Mar 26, 2020 Contributor

Describe the bug

When the `show_subdir_lastmod` option is enabled, ViewVC shows for directories in the directory view the log message of the most recently modified child thereof, along with the child file's name and revision number. Unfortunately, the child file's name is not properly HTML-escaped.

Steps to reproduce the behavior

1. In a CVS repository, copy the `,v` backing file for any non-dead versioned file into an otherwise empty subdirectory of the repository.

```
$ cd /opt/cvs/MyCVSRepository
$ mkdir new-module
$ cp some/existing/file.v 'new-module/<img src="#" onerror="alert(1)">.txt,v'
```

2. Ensure that `show_subdir_lastmod` is enabled in your `viewvc.conf` file (restarting any relevant servers).
3. In ViewVC, visit the parent directory of the newly created file. ViewVC will pass the name of your newly created file (minus the `,v` bit) to the browser without escaping that name for safe HTML transport. In this specific example, a JavaScript alert dialog will appear with the message "1".

Expected behavior

ViewVC should relay the name of the last-modified file, properly escaped.

cmpilato added the **bug** label on Mar 26, 2020

cmpilato added a commit that referenced this issue on Mar 26, 2020

`issue #211: escape CVS subdir last-modified file name` 64e7d5e

cmpilato added a commit that referenced this issue on Mar 26, 2020

`issue #211: escape CVS subdir last-modified file name` 1109c82

cmpilato added a commit that referenced this issue on Mar 26, 2020

`Add issue #211 fix to CHANGES.` 003a9fa

cmpilato added a commit that referenced this issue on Mar 26, 2020

`issue #211: escape CVS subdir last-modified file name` ad0f966

cmpilato added a commit that referenced this issue on Mar 26, 2020

`Add issue #211 fix to CHANGES.` ba51256

cmpilato commented on Mar 26, 2020 Contributor Author

Fixed in `master`; released in 1.2.1 and v1.1.28.

1

cmpilato closed this as completed on Mar 26, 2020

cmpilato added this to the **1.2.1** milestone on Mar 26, 2020

atoptsoglou commented on Mar 31, 2020

CVE-2020-5283 was assigned for this issue [1]

[1] https://github.com/viewvc/viewvc/blob/master/notes/SECURITY.md

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

1.2.1

Development

No branches or pull requests

2 participants