New issue

Jump to bottom

censor authorization part of headers before logging ReST API request #3248

Merged **migueldiascosta** merged 7 commits into `easybuilders:master` from `boegel:fix_token_log_leak` on Mar 16, 2020

Conversation 3 Commits 7 Checks 0 Files changed 5

boegel commented on Mar 16, 2020 • edited — Member

GitHub tokens were found to be "leaking" into the top-level log file when using `--from-pr` combined with `--debug`, as reported by **@zao**:

```
# relevant part of log for "eb --from-pr 10064 --debug"
== 2020-03-15 19:15:28,551 github.py:389 DEBUG Fetching easyconfigs from easybuilders/easybuild-easyconfigs PR #10064 into /tmp/eb-nqIFwJ/files_pr10064
== 2020-03-15 19:15:30,187 github.py:1843 INFO Successfully obtained GitHub token for user zao from keyring.
== 2020-03-15 19:15:30,188 rest.py:165 DEBUG cli request: GET, /repos/easybuilders/easybuild-easyconfigs/pulls/10064, None, {'Authorization': u'Token
deadbeefdeadbeefdeadbeefdeadbeefde', 'User-Agent': 'vsc-rest-client'}
== 2020-03-15 19:15:30,188 rest.py:207 DEBUG opening request:  https://api.github.com/repos/easybuilders/easybuild-easyconfigs/pulls/10064
== 2020-03-15 19:15:30,691 rest.py:177 DEBUG reponse len: 46
```

That's clearly not desirable, so the changes in this PR censor the `Authorization` part of the headers before the debug log statement.

To clarify the scope of this a bit:

- the log message only appears in the top-level log file, not in the individual software installation logs (see https://easybuild.readthedocs.io/en/latest/Logfiles.html);
  - as a consequence, tokens are *not* included in the partial log files that are uploaded into a gist when using `--upload-test-report` in combination with `--from-pr`, nor in the installation logs that are copied to the software installation directories;
- the message is only logged when using `--debug`, so it will not appear when using the default EasyBuild configuration (only `info` messages are logged by default);
- the log message is triggered via `--from-pr`, but also via various other GitHub integration options like `--new-pr`, `--merge-pr`, `--close-pr`, etc., but usually only appears in the temporary log file that is cleaned up automatically as soon as `eb` completes successfully;
- you may have several debug log files that include your GitHub token in `/tmp` (or a different location if you've set the `--tmpdir` EasyBuild configuration option) on the systems where you use EasyBuild, but they are located in a subdirectory that is only accessible to your account (permissions set to 700);
- the only way that a log file that may include your token could have been made public is if you shared it yourself, for example by copying the contents of the log file into a gist manually, or by sending a log file to someone;
- for log files uploaded to GitHub, your token would be revoked automatically when GitHub notices it (which is what happened to **@zao**)

We strongly encourage that you revoke the GitHub tokens you are using currently, via https://github.com/settings/tokens, and to replace them using a new token (using `eb --install-github-token --force`).

(this PR also includes the fixes from #3212 and #3226 which is required to get the full test suite to pass)

boegel added 3 commits 2 years ago

- `censor authorization part of headers before logging ReST API request` 37c805e
- `add test to check that --from-pr doesn't leak token in debug log` 379e9ba
- `fix broken test for --review-pr by using different PR to test with` a0f4162

boegel added the bug fix label on Mar 16, 2020

boegel added this to the **4.1.2** milestone on Mar 16, 2020

boegel added 2 commits 2 years ago

- `appease the Hound` e80d3b4
- `bump version to v4.1.2& update release notes` 482d03a

migueldiascosta approved these changes on Mar 16, 2020

View changes

migueldiascosta left a comment — Member

lgtm

Flamefire and others added 2 commits 2 years ago

- `Fix gitdb dependency on Python 2.6` 915782e
- `also include easybuilders#3212 in release notes for EasyBuild v4.1.2` a029a91

migueldiascosta approved these changes on Mar 16, 2020

View changes

migueldiascosta left a comment — Member

lgtm

migueldiascosta commented on Mar 16, 2020 — Member

Going in, thanks **@boegel**!

migueldiascosta merged commit `210743d` into `easybuilders:master` on Mar 16, 2020

---

boegel deleted the `fix_token_log_leak` branch 2 years ago

This was referenced on Mar 16, 2020

release EasyBuild v4.1.2 easybuilders/easybuild#609
Merged

sync develop with master after release of EasyBuild v4.1.2 #3249
Merged

censor authorization part of headers before logging ReST API request hpcugent/vsc-base#290
Merged

boegel mentioned this pull request on Oct 16, 2020

add support for using customized HTTP headers in download_file #3472
Merged

Reviewers

migueldiascosta ✓

Assignees

No one assigned

Labels

bug fix

Projects

None yet

Milestone

4.1.2

Development

Successfully merging this pull request may close these issues.

None yet

3 participants