New issue

Jump to bottom

Some Teampass files are available without authentication #2764

Closed **bstapes** opened this issue on Apr 2, 2020 · 2 comments

bstapes commented on Apr 2, 2020 • edited

Many of the files included in Teampass are available without authentication to anyone who can interact with the web server. While this may not be an issue for some of the images or Javascript files, it is an issue for the user-uploaded files that are available without authentication.

These include:

- upload dir - all file uploads (encrypted)
- avatars dir - all profile pictures
- backups dir - (presumably) Teampass backups
  - Note that accessing the scripts here can also trigger the backups to run
- files dir
  - PDFs generated via admin functions are saved here
- many files under the "includes" directory
- miscellaneous files under web root (license.md, changelog.txt, Dockerfile, etc)

Additionally, it does not appear that Teampass checks to see if directory listing is turned on on the web server. This feature is frequently on by default and when left on, makes it easy to discover the hashed file names that are sometimes used.

Steps to reproduce
Use a simple curl request to retrieve one of the files I noted above. EG:

```
curl http://<your teampass instance>/teampass/files/ldap.debug.txt
```

Steps to fix

- Review what files and directories should be exposed without authentication
- Ensure that only authenticated users can attempt to access files in sensitive directories (upload, backups, files, etc)
- Ensure that only authorized users can actually retrieve files in sensitive directories

Server configuration

Teampass version:
2.1.27.36

❤️ 1

huntr-helper commented on May 17, 2020

We have opened up a bounty for this issue on our bug bounty platform. Want to solve this vulnerability and get rewarded 💰 ? Go to https://huntr.dev/

👍 2

jamaisx commented on Aug 20, 2020

A few actions to mitigate:

1. Change $debugLdap to 0 in sources/identify.php to avoid create the debug file containing sensitive data
2. Protect "files" and "upload" folders (as suggested in configuration panel) moving them outside "htdocs"

nilsteampassnet closed this as completed on Oct 31

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants