New issue

Jump to bottom

open redirect for target_link_uri parameter #672

Closed **zandbelt** opened this issue on Sep 2, 2021 · 3 comments

zandbelt commented on Sep 2, 2021 Contributor

see #671, thanks **@Meheni**

Recently we have forged a URL for a phishing attack that redirects the user, after their authentication on our OP, to any site of our choice.

the forged url is as follows:

```
https://<oidc_callback>?iss=<issuer>&target_link_uri=https://FQDN_phishing\.<domain_your_oidc_callback>/
```

example:

```
https://myapplication.local/app/redirect_oidc?iss=<issuer>&target_link_uri=https://google.fr\.myapplication.local
```

After authentication, user is redirect to https://google.fr\.myapplication.loca

According to the OpenID Connect documentation,
https://openid.net/specs/openid-connect-core-1_0.html#ThirdPartyInitiatedLogin

> "target_link_uri
> OPTIONAL. URL that the RP is requested to redirect to after authentication. RPs MUST verify the value of the target_link_uri to prevent being used as an open redirector to external sites."

Does the module verify the value of the target_link_uri to prevent being used as an open redirector to external sites? and how to configure it in the module?

Meheni commented on Sep 2, 2021

Hi,
Thank you for your work.

Meheni

zandbelt closed this as completed in `03e6bfb` on Sep 3, 2021

zandbelt commented on Sep 3, 2021 Contributor Author

this fix is now included in release 2.4.9.4

Meheni commented on Sep 6, 2021

Hi,

I just tested the new version 2.4.9.4 and the fixed works very well.

I have the following message on my browser :

```
Error:

URL not allowed

Description:

value does not match the list of allowed redirect URLs: https://google.fr/.myapplication.local
```

Thank you again for your work.

Best regards,
Meheni

thalman pushed a commit to thalman/mod_auth_openidc that referenced this issue on Oct 29, 2021

`apply OIDCRedirectURLsAllowed setting to target_link_uri` ... ✓ `eac10ec`

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

 and others