New issue

Jump to bottom

FVP-02-005 WP1-3: Authenticationlistener allows disturbance of login #800

Closed **bakulf** opened this issue on Apr 7, 2021 · 0 comments

Labels p3

bakulf commented on Apr 7, 2021 • edited by data-sync-user Collaborator

It was found that Mozilla VPN in desktop environments sets up an HTTP server listening on a port acting as the OAuth callback expecting an Authorization Code to complete the Authentication of Mozilla VPN. This means there is a risk of attackers spamming requests to the local server via JavaScript, potentially disturbing the login process of the apps. This is possible as the local HTTP server is not protected by an additional secret and cannot distinguish between legitimate requests from malicious ones.

Affected File:
`src/tasks/authenticate/desktopauthenticationlistener.cpp`
Affected Code:

```
DesktopAuthenticationListener::DesktopAuthenticationListener(QObject* parent)
: AuthenticationListener(parent) {
MVPN_COUNT_CTOR(DesktopAuthenticationListener);
m_server = new QOAuthHttpServerReplyHandler(QHostAddress::LocalHost, this);
connect(m_server, &QAbstractOAuthReplyHandler::callbackReceived,
[this](const QVariantMap& values) {
logger.log() << "DesktopAuthenticationListener data received";
// Unknown connection.
if (!values.contains("code")) {
return;
}
QString code = values["code"].toString();
m_server->close();
```

It is recommended to protect the Authenticationlistener by a dynamically generated authentication token. The server should only be closed once authentication is either successfully completed or canceled by the user. By doing so, attackers cannot deny authentication by spamming and closing the listener prematurely. This should be feasible to implement as the Mozilla VPN already passes the local listener port to the HTTP login URL.

┆ Issue is synchronized with this Jira Task

bakulf added p3 **audit-issue** labels on Apr 7, 2021

bakulf self-assigned this on Apr 8, 2021

bakulf modified the milestone: **v2.2** on Apr 9, 2021

bakulf closed this as completed on Apr 9, 2021

data-sync-user unassigned **bakulf** on Aug 11, 2021

Assignees
No one assigned

Labels
p3

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant