huntr

Improper Authorization in cobbler/cobbler

0

✓ Valid Reported on Mar 2nd 2022

Description

When configuring cobbler-web to authentificate via PAM. The authorization of a account validity is missing. Therefore expired accounts can still login.

Proof of Concept

```
Enable authn_pam in the modules.conf

Create a testuser to login

    $ useradd expired_user

    $ passwd expired_user
    # 12345

    $ chage -E0 expired_user

Login via cobbler-web and see that it works although you don't have any pri
```

Impact

Since disabling an account still would allow login via ssh-keys or alike, it is common usage to expire an PAM account. Therefore the PAM library demands to check the handle with `pam_acct_mgmt()` after successful `pam_authenticate()`
After successfull authentication, the authorization of the user is not checked via `pam_acct_mgmt()` . This allows access to accounts that have been expired or h passwords. Both should be declined access by PAM convention. Depending configured this can become pretty severe. You don't revoke privileges for an account without a

reason.

References

- PAM pam_acct_mgmt manual

CVE
CVE-2022-0860
(Published)

Vulnerability Type
CWE-285: Improper Authorization

Severity
High (8.2)

Visibility
Public

Status
Fixed

Found by

ysf
@ysf
unranked

Fixed by

ysf
@ysf
unranked

This report was seen 611 times.

We are processing your report and will contact the **cobbler** team within 24 hours. 9 months ago

ysf submitted a patch 9 months ago

ysf 9 months ago

Chat with us

I'm open for adjustments on the CVE scoring. I think it's pretty difficult to estimate. I did in no

I'm open for adjustments on the CVE scoring. I think it's pretty difficult to estimate. I did in no way want to be rude or demanding.

ysf modified the report 9 months ago

We have contacted a member of the **cobbler** team and are waiting to hear back 9 months ago

A **cobbler/cobbler** maintainer 9 months ago Maintainer

Hi I acknowledge that I have read the bug report. I will try to confirm the bug until end of Monday (Berlin time).

If this bug is valid, not only cobbler-web is affected because the authentication is also used for the CLI and XMLRPC-API.

Enno G. 9 months ago Maintainer

Sorry I didn't sign in before. I am the upstream maintainer.

Enno G. 9 months ago Maintainer

The code we have is based upon a very old version of https://github.com/FirefighterBlu3/python-pam

I will try to check if a possible fix is to upgrade to a version of this library.

ysf 9 months ago Researcher

I'll check and will think about adding a report for python-pam also. Thank you

ysf 9 months ago Researcher

The current FirefighterBlu3/python-pam version has `pam_acct_mgmt()` in its build: FirefighterBlu3/python-pam/pam/internals.py

Enno G. 9 months ago

So this means switching to this library would solve the issue in your eyes?

Chat with us

ysf 9 months ago

Researcher

Yes, but my suggestion is to apply my patch/fix. Its‘s not a big change and would not need retesting as much as a new library would.

ysf submitted a patch 9 months ago

Enno G. 9 months ago

Maintainer

I do not see a patch on this webpage. Did I overlook something? Also I had internal plans to switch to this library as currently there is no PAM knowledge inside the Cobbler maintainers group present.

I fully agree that there are more risks involved, however I would love to still switch for reasons stated above. I hope that a dedicated library is better tested and maintained then our very old copy & pasted code from the original code (https://pypi.org/project/pam/).

ysf 9 months ago

Researcher

@admin can you help wo. The fix is not visible?

It‘s over here https://github.com/ysf/cobbler in the fix-pam branch. I completely Unterstand your decision tho.

A cobbler/cobbler maintainer 9 months ago

Maintainer

Okay I had a look. That fix is better then my idea indeed. Sadly you messed with the line endings which means the whole file is marked as a diff but I can fix that on my end.

Due to the fact that you pushed this to a public fork I would handle this as a public vulnerability now. Everyone can find and see your commit.

I will thus accept your report and we can go ahead and open the PR on upstream already. An embargo would not make sense because the commit is already public which describes the fix.

A cobbler/cobbler maintainer validated this vulnerability 9 months ago

ysf has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

ysf 9 months ago Researcher

I had to publish ist this way because huntr.dev asks for ist that way. I agree that this is stupid.

A cobbler/cobbler maintainer 9 months ago Maintainer

I am writing a pytest case which automatically checks that this is not happening. From your side I consider everything done, I will handle it from here on.

ysf 9 months ago Researcher

Thanks for the quick help!

Jamie Slome 9 months ago Admin

Hey all 👋

You should be able to see the submitted patch as part of the conversation feed. It is the second message in this chat thread.

You can directly click the hyperlink in that message to see the fix.

When you are ready (@maintainer) to confirm the fix against the report using the action button on the right side of the page, you will have an option to select @ysf as the fixer.

Let me know if you have any more questions, and happy to support you.

Jamie Slome 9 months ago Admin

I have also created this issue on our roadmap to address the creation of fixes publicly:

https://github.com/418sec/huntr/issues/2196

A cobbler/cobbler maintainer 9 months ago Maintainer

Okay I see now where the patch is but since this is not a comment but an acti
not identify this as accessible to me and thus skipped it. Thanks for the expla

Jamie Slome 9 months ago Admin

I have also created an issue on our public repository to address this as well! ^

https://github.com/418sec/huntr/issues/2197

Enno G. 9 months ago Maintainer

Since I can only confirm the fix once it is published in the repo I have created https://github.com/cobbler/cobbler/security/advisories/GHSA-mcg6-h362-cmq5 to coordinate the efforts until that is the case. The reporter has been added to the GH Security Vulnerability Draft linked above.

We have sent a fix follow up to the **cobbler** team. We will try again in 7 days. 9 months ago

Enno G. 9 months ago Maintainer

I believe I have problems with my environment. I asked for help from a colleague who is firm with this matter.

Jamie Slome 9 months ago Admin

Is there anything we can do to support here?

Enno G. marked this as fixed in **3.3.2** with commit **9044aa** 9 months ago

ysf has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Enno G. 9 months ago Maintainer

Nope all fine. Everything was fixed as expected now.

Jamie Slome 9 months ago Admin

Great 👍

Sign in to join this conversation

Chat with us