# Improper Authorization and possible DoS when using PAM Auth in bareos/bareos

0

Valid Reported on Mar 6th 2022

## Description

When bareos versions after 18.2 are build and configured for PAM authentification it skips checking authorization completely. Expired accounts and accounts with expired passwords can still login. Further after wrong authentication or the code returns without releasing the PAM handle, thus assigning memory without releasing it.

## Proof of Concept

You can expire an account with `chage -E0 <username>` and still login.

## Impact

Since disabling an account in PAM still allows to login via ssh-keys, it's common to set accounts to expire if you want to deny access. So accounts who technically don't have any privilege are still allowed to login. To circumvent this, after an successful call to `pam_authenticate` it is necessary to call `pam_acct_mgmt` for authorization purposes. Because of not releasing the PAM memory after unsuccessful tries, it is theoreticaly possible to occupy memory resulting in a DoS.

## References

- C3H2-CTF

CVE
CVE-2022-24755
(Published)

Vulnerability Type
CWE-285: Improper Authorization

Severity

Severity
High (8.1)

Visibility
Public

Status
Fixed

Found by

ysf
@ysf
unranked

Fixed by

ysf
@ysf
unranked

This report was seen 515 times.

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

**ysf** modified the report 9 months ago

**ysf** modified the report 9 months ago

**ysf** submitted a **patch** 9 months ago

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

**Andreas Rogge** modified the report 9 months ago

**ysf** submitted a **patch** 9 months ago

**Andreas Rogge** 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

@admin I wouldn't request a CVE for the authorization issue here, but for the potential DoS I'll let @maintainer decide

Andreas Rogge 9 months ago Maintainer

We're going to handle this as two separate problems and we would like a CVE number for both of them.
However, I can also just order the CVE-Numbers via GitHub if that's OK for you.

ysf 9 months ago Researcher

Yeah sure, if that's your process anyway I don't mind. - @admin can you assign cves to this report afterwards?

Andreas Rogge 9 months ago Maintainer

FYI: there is now a PR with a fix at https://github.com/bareos/bareos/pull/1115

Jamie Slome 9 months ago Admin

Absolutely, we can assign a CVE for this. Can I just confirm that a CVE has not already been requested from GitHub, just to prevent duplication of CVEs? Once I get your confirmation @arogge, I will assign a CVE to the report.

Andreas Rogge 9 months ago Maintainer

@admin In the meantime I have requested CVEs for both issues at GitHub (I may have misunderstood the ysf's comment). If you could add the CVE numbers to this report, after they're issued, that would be great!

ysf 9 months ago Researcher

@admin due to improper disclosement in my part - I put two topics in one report - we know have two CVEs. Should I add another one or can you add two CVEs afterward

Jamie Slome 9 months ago Admin

@maintainer @ysf - no worries 👍 Let me know the IDs once you have them!

We can attach a single CVE from a UI perspective, but we will just make the other CVE number visible in the comments section.

ysf 9 months ago Researcher

@admin Andreas wrote me that he can't choose myself for the fix bounty. Do you know if there is any technical issue? Maybe because his refactoring cleaned other lines that I mentioned?

Having one makes a difference community wise as I assume it'll be one cve, vulnerbility, fix and bounty on my stats - That said, it is truely ok for me to do so since I'm doing this for the bigger picture. There might be a use case for the other researchers tho, especially when there is a bigger bounty involved.

Andreas Rogge 9 months ago Maintainer

@admin we got Numbers:
CVE-2022-24755 for the Authorization
CVE-2022-24756 for the DoS

Andreas Rogge 9 months ago Maintainer

@ysf turns out I cannot read properly: I can select who's going to get the fix bounty at the bottom of the "Confirm Fix" form. As always you just have to read till the end...

However, what seems to be not possible is to mention multiple fixes. We're going to fix these issues for all supported releases, which I would like to document here, too.
Maybe @admin can tell me how to proceed in this case?

Jamie Slome 9 months ago Admin

I'd recommend that we use the CVE and fix for the Improper Authorization issue, and then can just keep the CVE and commit references for the DoS issue in the comments section here.

@arogge - feel free to confirm fix using the commit SHA that addresses the Improper Authroziation, and could you please let me know which CVE is being used fo

Andreas Rogge 9 months ago Maintainer

@admin the Authorization issue has CVE-2022-24755.
My Problem with the commit SHA is, that there will be four of these: one for the development branch and one for each of our maintenance branches.

Jamie Slome 9 months ago Admin

I see - perhaps we can use the commit SHA that is merged into your main branch, used for releases - i.e. a merge commit SHA with all included?

Andreas Rogge 9 months ago Maintainer

If it was just that simple... I'll go with just the master-commit.

Jamie Slome 9 months ago Admin

Okay 👍

It sounds like we could definitely benefit from a new feature here, around attaching multiple fix commits?

If you feel strongly about this, I'd love to invite you to create a GitHub Issue our on public repo where we track feature requests:

Create feature request

Andreas Rogge 9 months ago Maintainer

I wrote a FR, see https://github.com/418sec/huntr/issues/2201

We have sent a fix follow up to the **bareos** team. We will try again in 7 days. 8 months ago

**Andreas Rogge** marked this as fixed in **21.1.0** with commit **e3855b** 8 months ago

**ysf** has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation





Chat with us