huntr

# Improper Authorization in clusterlabs/pcs

0

✓ Valid Reported on Mar 7th 2022

## Description

Pacemakers daemon pcsd allows authentication via PAMs `pam_authenticate` . Unfortunately the authorization via `pam_acct_mgmt` has been omitted. Therefore unprivileged expired accounts that have been denied access can still login.

## Proof of Concept

You can expire an account with `chage -E0 <username>`

## 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 here. This also counts for accounts with expired passwords. A fix is supplied in the report.

## References

- C3H2-CTF

CVE
CVE-2022-1049
(Published)

Vulnerability Type
CWE-285: Improper Authorization

Severity
Medium (6.5)

Visibility
Public

Chat with us

Status

Fixed

Found by

ysf

@ysf

unranked

Fixed by

ysf

@ysf

unranked

This report was seen 1,210 times.

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

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 9 months ago

ysf submitted a patch 9 months ago

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

A **clusterlabs/pcs** maintainer 9 months ago Maintainer

Hi @ysf,

Thank you for reaching out and reporting this issue. I have contacted our internal security team to review it and assess its severity. I'll get back to you and confirm the vulnerability when I hear from them.

Regards,
Tomas

We have sent a follow up to the **clusterlabs/pcs** team. We will try again in 7 d

Chat with us

A **clusterlabs/pcs** maintainer has acknowledged this report 8 months ago

A clusterlabs/pcs maintainer modified the report 8 months ago

A clusterlabs/pcs maintainer validated this vulnerability 8 months ago

ysf has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

ysf 8 months ago Researcher

Hey, will do when github works again. Currently my repository throws 500 errors back and forth.

ysf 8 months ago Researcher

@admin I can't choose the repository since it is named differently (pcs-1) than the original project name.

Jamie Slome 8 months ago Admin

Hello @ysf 👋

Are you trying to submit a fix?

ysf 8 months ago Researcher

@Yes - It's already in my branch pcs-1 and a PR in the clusterlabs/pcs repository.
@maintainer will you assign a CVE through redhat to this issue?

ysf 8 months ago Researcher

Gna. I meant @admin of course.

A clusterlabs/pcs maintainer 8 months ago Maintainer

@ysf I'm not in charge of the CVE process, but I forwarded your question to R
team.

Chat with us

Jamie Slome 8 months ago Admin

@maintainer - with regards to the CVE, we are happy to assign and publish a CVE on your behalf if you would like?

@ysf - with regards to the fix, it seems like a bug in our UI preventing you from selecting a differently named fork.

Can you please confirm the name of the branch, and I will deal with patch submission on my end on your behalf? 👍

ysf 8 months ago Researcher

@admin it's https://github.com/ysf/pcs-1/tree/fix_pam_authorization

Thank you

Jamie Slome 8 months ago Admin

It doesn't look like there is a diff yet?

https://github.com/ClusterLabs/pcs/compare/main...ysf:fix_pam_authorization

A **clusterlabs/pcs** maintainer 8 months ago Maintainer

@admin I just merged the fix by @ysf

ysf 8 months ago Researcher

Exactly, there is no diff because it already has been merged. You can see the reference to huntr.dev in the CHANGELOG.md

Jamie Slome 8 months ago Admin

In any case, it doesn't actually matter, as we just request the patch to be able to share the diff URL with the maintainer in the comments section.

@maintainer - you can still proceed to `confirm fix` and select @ysf as the fixer in the dropdown as a patch has still been submitted and recorded 👍

Chat with us

We will just need to address this minor bug :)

A **clusterlabs/pcs** maintainer marked this as fixed in **0.11.3 and 0.10.14** with commit **fb8600**
8 months ago

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

This vulnerability will not receive a CVE ✗

Jamie Slome 8 months ago Admin

Would you like us to assign and publish a CVE for this report?

A **clusterlabs/pcs** maintainer 8 months ago Maintainer

CVE-2022-1049 has been assigned for this issue.

Jamie Slome 8 months ago Admin

I have added the CVE to the report 👍

Sign in to join this conversation

2022 © 418sec

leaderboard

FAQ

contact us

terms

privacy policy

team

Chat with us