huntr

# Improper Authorization in gogs/gogs

0

✓ Valid Reported on Mar 6th 2022

## Description

When Gogs is build and configured for PAM authentification it skips checking authorization completely. Therefore expired accounts and accounts with expired passwords can still login.

## 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 whom have been privilege revoked are still able to login.

## Occurrences

pam.go L29

Here's a patch since I don't want to make this public in a repository.

```
--- a/internal/auth/pam/pam.go
+++ b/internal/auth/pam/pam.go
@@ -26,5 +26,9 @@ func (c *Config) doAuth(login, password string) error
                return err
        }

-       return t.Authenticate(0)
+    if err = t.Authenticate(0); err != nil {
+           return err
+    }
+
+
+        return t.AcctMgmt(0)
 }
```

## References

- pam_acct_mgmt manpage

CVE
CVE-2022-0871
(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 603 times.

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

@admin The gogs team is still working on the other issue they're frozen for. What is the freeze/unfreeze process? Can't find it in the FAQs and sure would like bounty if possible.

ysf modified the report 9 months ago

ysf 9 months ago Researcher

A similar bug has been reported to Gitea, we should coordinate publishing them after both repositories have been fixed.

ysf 9 months ago Researcher

Gogs have been contacted according to their security.md here:
https://github.com/gogs/gogs/issues/6810

Joe Chen validated this vulnerability 9 months ago

ysf has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Jamie Slome 9 months ago Admin

@ysf - the prize pot is frozen whilst the entire pot is being consumed by another pending report. Once the report has been reviewed that consumes the entire prize pot, 30 days will elapse before the prize pot refills again.

Created this issue here to help address this better! Feel free to leave your thoughts on the issue too.

ysf submitted a patch 9 months ago

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

Joe Chen marked this as fixed in 0.12.5 with commit 64102b 9 months ago

Chat with us

ysf has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

pam.go#L29 has been validated ✓

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us