Gogs Ownage

Backdooring source code at scale.

TheZero

@ToHack - 02/2019

TOHack

What is Gogs

What is Gogs

TOHack

What is Gogs

Gogs is a painless self-hosted Git service.

- Written in Go
- Multiplatform
- Previously called Gogit
- Use Sqlite3, support Postgres / MySQL / MariaDB, etc.
- It's Hipster

TOHack

So, what’s wrong with Gogs?

2 Law of Gogs

- Sessions are stored on file, unsigned and unencrypted
- A Gogs admin can always perform RCE with Git Hooks

TOHack

The data folder

TOHack

The Magic session file

Gob is a Go specific serialization method. It has support for all Go data types except for channels and functions. Gob also encodes the type information into the serialized form.

```
~ > R > gogs > go run sess.go                                    11:07:00
map[uname:administrator uid:1]
~ > R > gogs > xxd payload                                       11:07:22
00000000: 0eff 8104 0102 ff82 0001 1001 1000 0044  ...............D
00000010: ff82 0002 0673 7472 696e 670c 0700 0575  .....string....u
00000020: 6e61 6d65 0673 7472 696e 670c 0f00 0d61  name.string....a
00000030: 646d 696e 6973 7472 6174 6f72 0673 7472  dministrator.str
00000040: 696e 670c 0500 0375 6964 0569 6e74 3634  ing....uid.int64
00000050: 0402 0002                                ....
```

TOHack

Git Hooks!

Execute shell command when a git event is triggered

- Repository specific settings
- Available events: pre-receive, update, post-receive
- RCE whenever someone makes a commit

TOHack

RCE whenever someone makes a commit

TOHack

CVE-2018-18925

Unauthenticated PrivEsc (then RCE) via Path Traversal in the `i_like_gogit` cookie loading the admin session file.

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 9.8 CRITICAL

Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3 legend)

Impact Score: 5.9

Exploitability Score: 3.9

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): None

User Interaction (UI): None

Scope (S): Unchanged

Confidentiality (C): High

Integrity (I): High

Availability (A): High

TOHack

CVE-2018-20303

Authenticated PrivEsc (then RCE) via Path Traversal by uploading a repository file in the session folder.

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 7.5 HIGH

Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N (V3 legend)

Impact Score: 3.6

Exploitability Score: 3.9

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): None

User Interaction (UI): None

Scope (S): Unchanged

Confidentiality (C): None

Integrity (I): High

Availability (A): None

TOHack

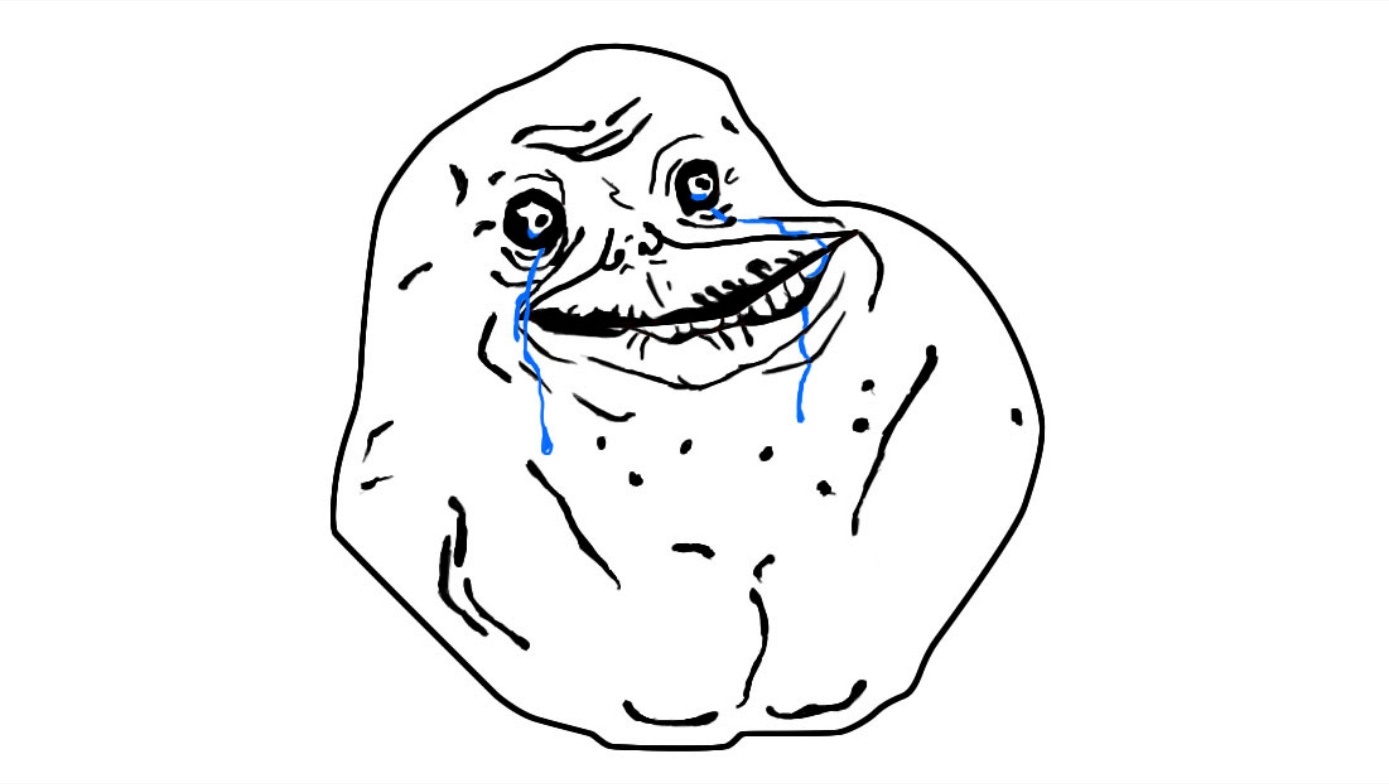
...

- (Low) Unauthenticated file upload
- (Low) File upload filter bypass
- ...
- ...

TOHack


gogs / gogs
Watch 1,082
Unstar 29,058
Fork 3,343
Code
Issues 613
Pull requests 18
Wiki
Insights
Upload Release Attachment without a valid repo/release /account #5599
Edit
New issue
Open
TheZ3ro opened this issue 10 days ago · 0 comments
TheZ3ro commented 10 days ago
Describe the bug
It's possible to upload a release attachment file without having a valid repository/release and without a valid user account, even if DISABLE_REGISTRATION is set to true in the app.ini configuration file.
The bug/vulnerability is not present if REQUIRE_SIGNIN_VIEW is set to true since all the requests will reply with a 302 redirect to the login page.
Assignees
No one assigned
Labels
None yet
Milestone

...



TOHack

Some Data

LiVe DeMo On GiT.LsD.CaT

GogsOwnz.py still in progress.

Stay Tuned ;)

Domande? (non troppo scomode :)