huntr

Open Redirect on login in go-gitea/gitea

0

✓ Valid Reported on Mar 23rd 2022

Description

Although https://github.com/go-gitea/gitea/pull/9678 protects against most open redirects there is an unfortunate flaw in its logic due to browser behaviour when presented with Locations that have backslashes in them

Proof of Concept

```
https://try.gitea.io/user/login?redirect_to=/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\the
```

Following a succesful login using this url, a redirect will be sent back to the browser with the Location header equal to: `/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\thedailywtf.com` . This will be interpreted by the browser as a redirect to `//thedailywtf.com` .

Impact

This vulnerability constitutes an open redirect:

Users may be redirected to an untrusted page that contains malware which may then compromise the user's machine. This will expose the user to extensive risk and the user's interaction with the web server may also be compromised if the malware conducts keylogging or other attacks that steal credentials, personally identifiable information (PII), or other important data.

Users may be subjected to phishing attacks by being redirected to an untrusted page. The phishing attack may point to an attacker controlled web page that appears to be a trusted web site. The phishers may then steal the user's credentials and then use these credentials to access the legitimate web site.

Mitigation

Chat with us

This vulnerability will be mitigated with:

This vulnerability will be mitigated with:
https://github.com/go-gitea/gitea/pull/19175

CVE
CVE-2022-1058
(Published)

Vulnerability Type
CWE-601: Open Redirect

Severity
High (7.2)

Visibility
Public

Status
Fixed

Found by

zeripath
@zeripath
maintainer

Fixed by

zeripath
@zeripath
maintainer

This report was seen 934 times.

We are processing your report and will contact the **go-gitea/gitea** team within 24 hours. 8 months ago

A **go-gitea/gitea** maintainer has acknowledged this report 8 months ago

zeripath submitted a patch 8 months ago

Jamie Slome 8 months ago

Chat with us

@zeripath - I can see that you are trying to validate this report. We do currently have protections

@zeripath - I can see that you are trying to validate this report. We do currently have protections in place to prevent maintainers from validating their own reports but recognise that this is a feature that maintainers do want.

Would you like me to go ahead and approve this report and confirm the fix?

Jamie Slome 8 months ago Admin

I've also created this public feature request to keep track of the progress of this.

zeripath 8 months ago Researcher

The PR hasn't been merged yet - so I guess once it's merged it should be considered fixed.

Jamie Slome 8 months ago Admin

Sure 👍 Would you like me to approve the report in the meantime? This will not make the report public. The report goes public only once the fix is confirmed.

zeripath 8 months ago Researcher

yes please approve.

Jamie Slome validated this vulnerability 8 months ago

zeripath has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Jamie Slome 8 months ago Admin

Sorted 👍 Once you are ready with the fix, let me know, and I will confirm this too.

zeripath 8 months ago Researcher

fix is in https://github.com/go-gitea/gitea/commit/e3d8e92bdc67562783de9a76b5b7842b68daeb48 on relea zeripath 8 months ago Researcher

@admin the fix for this has been released as part of 1.16.5

Jamie Slome marked this as fixed in **1.16.5** with commit **e3d8e9** 8 months ago

zeripath has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Jamie Slome 8 months ago Admin

Sorted! 👍

Sign in to join this conversation

privacy policy

Chat with us