Stored xss bug in gogs/gogs

Valid Reported on Apr 12th 2022

0

Description

stored xss bug

Proof of Concept

create a public repo and create a issue .
now in issue upload a html file with xss payload inside.
When any user view the repo and click the attachment link then xss is executed .
you can upload https://github.com/ranjit-git/poc/edit/master/evilsvgfile.svg this file also

VIDEO

https://drive.google.com/file/d/11wxTj8ILFLxRe2uoAvQ_39i7Hqa1tWHI/view?usp=sharing

Impact

As the repo is public , any user can view the report and when open the attachment then xss is executed. This bug allow executed any javascript code in victim account .

CVE
CVE-2022-1464
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
High (7.3)

Registry
Packagist

Affected Version

0.12.6

Visibility
Public

Status
Fixed

Found by

ranjit-git
@ranjit-git
amateur

This report was seen 832 times.

We are processing your report and will contact the **gogs** team within 24 hours. 7 months ago

ranjit-git modified the report 7 months ago

We have contacted a member of the **gogs** team and are waiting to hear back 7 months ago

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

We have sent a second follow up to the **gogs** team. We will try again in 10 days. 7 months ago

Joe Chen validated this vulnerability 7 months ago

ranjit-git has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

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

Joe Chen 7 months ago Maintainer

The patch has landed in
https://github.com/gogs/gogs/commit/cb35b73048b91ca32ee89d5b05a09552
will only "Mark as fixed" until a new release is published according to security
(https://github.com/gogs/gogs/blob/main/SECURITY.md).

Joe Chen marked this as fixed in 0.12.7 with commit bc7744 7 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Joe Chen 7 months ago Maintainer

The patch has been published, thanks again for finding this vulnerability!

Sign in to join this conversation