

## Improper Privilege Management in delgan/loguru

0

 Valid

Reported on Jan 11th 2022

### BUG

unprivileged user can see log file and sensitive information disclosed

### SUMMARY

loguru create log file to store the log . Log may contain many sensitive information like username,password,token,key etc .

So, this log file should not be accessed by other user .

But when loguru create log file then file permission is `-rw-rw-r-- 1 user user 345 Jan 11 14:47 combined.log` which can be accessed by any user.

In linux system there may be many users with different privileges . but any user can see this log file .

### STEP TO REPRODUCE

run below code

```
from loguru import logger
data="Data to be logged , password123 is incorrect" #sensitive data logging
logger.add("combined.log") #creating log file with insecure permission
logger.info(data)
```

Now a `combined.log` file will be created with all log information . check file permission

```
user@user-xx:~$ ls -lh combined.log
-rw-rw-r-- 1 user user 345 Jan 11 14:47 combined.log
```


[Chat with us](#)

So, this file has read permission for all system user . Thus any user can read this log file .I see mostly all webserver , logger etc log there info in a file and it is only accessed by current user who created the file . But in this case it has read permission for all user .

## SUGGESTED FIX

You should change the logfile permission to be access only by current user who crated the file or sudo user .

## Occurrences

-  \_file\_sink.py L16-L372
-  \_logger.py L75-L1900

### CVE

CVE-2022-0338

(Published)

### Vulnerability Type

CWE-269: Improper Privilege Management

### Severity

Medium (4.3)


### Visibility

Public

### Status

Fixed

### Found by



ranjit-git

@ranjit-git

amateur ✓

This report was seen 479 times.

We are processing your report and will contact the **delgan/loguru** team within 24 hours.  
a year ago

We have contacted a member of the **delgan/loguru** team and are waiting  
10 months ago

Chat with us

delgan 10 months ago

Maintainer

Hi.

Loguru uses the same default permissions as any other Python logging library (especially the standard one).

However, one can easily configure Loguru to use the preferred file permissions:

```
def opener(file, flags):  
    return os.open(file, flags, 0o600)  
  
logger.add("combined.log", opener=opener)
```

Loguru is perfectly secure to use. I'll add a word in the documentation about that.

ranjit-git 10 months ago

Researcher

Thanks for reply.  
Can you plz change the report status by validating it.

ranjit-git 10 months ago

Researcher

```
def opener(file, flags):  
    return os.open(file, flags, 0o600)  
  
logger.add("combined.log", opener=opener)
```

Don't know that there is handler for changing the permission.  
But default permission 600 would be better because most of users don't change the file permission manually.  
Thanks again

We have sent a follow up to the delgan/loguru team. We will try again in 7 days. 10 months ago

delgan 10 months ago

Maintainer

Chat with us

Hi @ranjit-git.

I'm not sure I should validate the security report, because that would acknowledge that Loguru contains CWE-269 weakness, right?

This is an issue qualified as "High Severity" yet we both agreed that Loguru does not contain such issue per se. I'm afraid it will confuse the user into thinking that Loguru is not secure.

Can the severity be somehow lowered?

ranjit-git modified the report 10 months ago

ranjit-git 10 months ago

Researcher

@maintainer

I just lowered the severity to 5.4 .

Is this ok?

ranjit-git modified the report 10 months ago

ranjit-git 10 months ago

Researcher

Sorry it's 4.3 severity now

ranjit-git 10 months ago

Researcher

Hi @maintainer

any update?

delgan validated this vulnerability 10 months ago

ranjit-git has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

delgan 10 months ago

Sorry for the delay and thanks for lowering the severity. ;)

Chat with us

delgan marked this as fixed in 0.5.3 with commit [ea3937](#) 10 months ago

The fix bounty has been dropped ❌

This vulnerability will not receive a CVE ❌

\_file\_sink.py#L16-L372 has been validated ✅

\_logger.py#L75-L1900 has been validated ✅

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us