

Session Fixation in filegator/filegator

0



Valid

Reported on May 22nd 2022



Requirements

None.



Description

The `updateUser` function does not reset user's session.



Proof of Concept

Use two browsers and on the first, update the second user's session to delete his privileges.



Files Users Admin Log out

+ New

No pagination

Name ↓	Username	Permissions	Role
test	test		User
Guest	guest		Guest
Admin	admin	read, write, upload, download, batchdownload, zip	Admin

Going to the second, you and refreshing the page, you will that the user have lost his right (until his session get over).



test Log out

Home



+ New

No pagination



Name ↑

Size



I steal can see it

Folder

22/05, 11:11:11

Chat with us

Impact

Due to this vulnerability, it won't be possible to properly handle rights management.

CVE

CVE-2022-1849

(Published)

Vulnerability Type

CWE-384: Session Fixation

Severity

Medium (4.3)

Registry

Other

Affected Version

*

Visibility

Public

Status

Fixed

Found by



Mizu

@kevin-mizu

pro



Fixed by



Milos Stojanovic

@alcalbg

maintainer

This report was seen 527 times.

We are processing your report and will contact the **filegator** team within 24 hours.

Chat with us

We have contacted a member of the **filegator** team and are waiting to hear back 6 months ago

Milos Stojanovic validated this vulnerability 6 months ago

Mizu has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Milos Stojanovic marked this as fixed in **7.8.0** with commit **fcd399** 6 months ago

Milos Stojanovic has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

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

[Chat with us](#)