

Path Traversal in prasathmani/tinyfilemanager

0



Valid

Reported on Feb 15th 2022

Description

A Path Traversal vulnerability exists in Tiny File Manager, which allows the upload of files to an arbitrary location in the server. This flaw derives from the way that the file upload/creation is handled when a file with the same name already exists in the target directory.

Affected Code Snippet

```
// tinyfilemanager.php
// ... snippet ...
if(file_exists ($fullPath) && !$override_file_name) {
    $ext_1 = $ext ? '.'.$ext : '';
    $fullPath = str_replace($ext_1, '', $fullPath) .'_'. date('ymdHis').
}
// ... snippet ...
```

If we look at how `str_replace` is used to separate the old filename from its extension, we can see that it will in fact remove all occurrences of the extension from the whole fullpath parameter. Therefore, if an attacker sends, for example, two consecutive requests with fullpath `...php/...php/...php/...php/...php/var/www/html/benign.php` and filename `shell.php`, it will move the uploaded file to `../../../../../../../../var/www/html/benign_<DATE>.php`.

Proof of Concept

```
curl -s -H 'Cookie: filemanager=<SESSIONID>' -F'file=@shell.php' -F'fullpat
curl -s -H 'Cookie: filemanager=<SESSIONID>' -F'file=@shell.php' -F'fullpat
```

[Chat with us](#)

Impact

By leveraging this vulnerability to upload a webshell, it's possible to achieve RCE in the server/container.

CVE

CVE-2022-1000

(Published)

Vulnerability Type

CWE-22: Path Traversal

Severity

High (8.8)


Visibility

Public

Status

Fixed

Found by




joaogmauricio

@joaogmauricio

unranked ▾

Fixed by



joaogmauricio

@joaogmauricio

unranked ▾

This report was seen 852 times.

We are processing your report and will contact the **prasathmani/tinyfilemanager** team within 24 hours. 9 months ago

We have contacted a member of the **prasathmani/tinyfilemanager** team and we will hear back 9 months ago

We have sent a follow up to the **prasathmani/tinyfilemanager** team. We will try again in 7 days

Chat with us

we have sent a follow up to the **prasathmani/tinyfilemanager** team. We will try again in 7 days.
9 months ago

We have sent a second follow up to the **prasathmani/tinyfilemanager** team. We will try again in
10 days. 9 months ago

We have sent a third and final follow up to the **prasathmani/tinyfilemanager** team. This report
is now considered stale. 9 months ago

Prasath Mani validated this vulnerability 9 months ago

joaogmauricio has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Prasath Mani marked this as fixed in **2.4.7** with commit **154947** 9 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Prasath Mani 9 months ago Maintainer

@joaogmauricio, thanks reporting.

Jamie Slome 9 months ago Admin

@prasathmani - thanks for your contributions and effort here! Are you happy for us to assign
and publish a CVE for this report?

Jamie Slome 9 months ago Admin

@prasathmani - can we also confirm that @joaogmauricio did fix the vulnerability so that we
can appropriately represent this on the report and their user profile?

Prasath Mani 8 months ago Maintainer

@Jamie, @joaogmauricio - has fixed the issue and CVE report is not required.

Jamie Slome 8 months ago Admin

Chat with us

Just for clarity, @joaogmauricio has explicitly requested a CVE - are you happy to publish one, or would you prefer not to?

joaogmauricio 8 months ago

Researcher

Hi @Jamie, thank you very much for your support and for bringing some clarity. Just to be even more clear, the CVE request process would *not* bring any extra work for @Prasath, correct?

Jamie Slome 8 months ago

Admin

Correct - we will do all the work! 👍

Prasath Mani 8 months ago

Maintainer

if CVE is required, please go ahead

Jamie Slome 8 months ago

Admin

CVE assigned and published 🎉

joaogmauricio 8 months ago

Researcher

🎉🎉🎉 Thank you very much Prasath and Jamie for your full support. :)

Last question to Jamie (hopefully): how do we stand in regards to the fix attribution? Thanks.

Jamie Slome 8 months ago

Admin

Also sorted 👍

joaogmauricio 8 months ago

Researcher

I still see a 0 there, but that's maybe some sort of caching issue. I'll wait some not, I'll open a ticket as per your suggestion. Thanks once again and have a g.

Chat with us

Jamie Slome [8 months ago](#)

[Admin](#)

It was a small bug on our side - deploying a fix for it now 🐞

joaogmauricio [8 months ago](#)

[Researcher](#)

:) Thanks!

Sign in to join this conversation

2022 © 4l8sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 4l8sec

company

about

team

Chat with us