

External Control of File Name or Path in netristv/ws-scrpcy 0

Valid

Reported on Dec 12th 2021

Description

read file From server

Proof of Concept

GET ../../../../../../../../../../../../../../etc/passwd HTTP/1.1
Host: xxxx

Impact

test on ws-scrpcy-0.7, this is The latest version

CVE
CVE-2021-3845
(Published)


Vulnerability Type
CWE-73: External Control of File Name or Path

Severity
None (0)

Visibility
Public

Status
Fixed

Found by



whoamisky

@whoamisky

unranked

This report was seen 627 times.

We are processing your report and will contact the **netristv/ws-scrpcy** team within 24 hours.
a year ago

We created a **GitHub Issue** asking the maintainers to create a SECURITY.md a year ago

Sergey Volkov a year ago

Maintainer

@whoamisky Thank you for the report.

This method is only used to read the configuration file.
User (admin/service owner) should pass path to the file in **WS_SCRPCY_CONFIG** environment variable.
The content of the file is not avalivale to end users over HTTP.

Sergey Volkov has invalidated this vulnerability a year ago

See comment.

The disclosure bounty has been dropped ❌

The fix bounty has been dropped ❌

Sergey Volkov a year ago

Maintainer

@admin Can we please reopen this report and change its status?

Jamie Slome a year ago

Admin

@drauggres - sure, we can arrange that for you!

Would you like me to change it back to **pending** so that you can re-mark it as valid?

Sergey Volkov a year ago

Maintainer

Yes please.

P.S. [Not related to this report] The link from email notification brought me to www.huntr.dev and I am not authorized there, but I still have the active session on huntr.dev (maybe you have some problem with cookie)

Jamie Slome a year ago

Admin

Will get this sorted for you now!

With regards to the cookie issue, I have created a bug ticket internally, and we will investigate the problem shortly! Thank you for letting us know ♥

Jamie Slome a year ago

Admin

For reference, I have now set the report back to [pending](#) as requested by @drauggres.

Thanks! 🙏

Sergey Volkov validated this vulnerability a year ago

whoamisky has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Sergey Volkov marked this as fixed in v0.7.1 with commit [e83cf6](#) a year ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

whoamisky a year ago

Researcher

@admin you can give me a CVE ?

Jamie Slome a year ago

Admin

Before we assign a CVE, we just need to get confirmation from the maintainer that they are happy for us to create one (require maintainer confirmation when our system doesn't automatically assign and publish one).

@drauggres - are you happy for us to assign a CVE to this vulnerability report?

Sergey Volkov a year ago

Maintainer

I don't mind.

whoamisky a year ago

Researcher

@drauggres tks

Jamie Slome a year ago

Admin

CVE published! 🎉

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

part of 418sec

company

about

team

