huntr

Path Traversal in getgrav/grav

0

✓ Valid Reported on Oct 28th 2021

Steps:

Host the project locally.
For example if address is http://127.0.0.1:8088 ==> visit
http://127.0.0.1:8088/system/config/permissions.yaml
http://127.0.0.1:8088/system/config/permissions.yaml ==> you will get the content of permissions.yaml file.

Impact:

Successful exploitation could allow an attacker to traverse the file system to access files or directories that are outside of restricted directory on the remote server. This could lead to the disclosure of sensitive data on the vulnerable server.

References

- https://www.cvedetails.com/cve/CVE-2021-42261/

CVE
CVE-2021-3924
(Published)

Vulnerability Type
CWE-22: Path Traversal

Severity
High (8.8)

Visibility
Public

Status
Fixed

Found by

takester
@takester
unranked

Fixed by

Matias Griese
@mahagr
maintainer

This report was seen 447 times.

We have contacted a member of the **getgrav/grav** team and are waiting to hear back a year ago

A **getgrav/grav** maintainer a year ago

I cannot reproduce this as htaccess block access to any yaml file.

Are you using some other server?

takester a year ago Researcher

Yes, I am using apache

takester a year ago Researcher

Actually I have setup it in my kali machine and using the document provided in GitHub repo.

takester a year ago Researcher

And ran the application same.

A **getgrav/grav** maintainer a year ago

Chat with us

Maybe your installation doesn't allow .htaccess file in the site? Though that would render the site unusable as pages would not work...

I cannot access the files in any site, here's an example:
https://getgrav.org/system/config/permissions.yaml

Also
https://github.com/getgrav/grav/blob/develop/.htaccess#L62

That line prevents anyone from accessing the yaml files.

takester a year ago Researcher

Yes the filter seems to be right for the directories (For System and Vendor)
https://github.com/getgrav/grav/blob/develop/.htaccess#L62

But still we can able to access file inside the other folders (backup,bin,cache...)

And about the installation, I have followed the same method as mentioned in GitHub repo, so it must be in code logic fault if it is being installed in linux or so. Please check it and let me know.

Steps that I followed for installation.

```
git clone https://github.com/getgrav/grav.git

cd grav

bin/grav install
```

A getgrav/grav maintainer a year ago

Access to all files are blocked for backup, cache, bin and so on:

https://github.com/getgrav/grav/blob/develop/.htaccess#L60

I just verified it works for arbitrary file in those locations.

takester a year ago Researcher

Then what is the issue, because I followed the steps exactly as mentioned.
And we don't have to manually change anything (htaccess) after installing, Right??
Please try to setup it locally as I set up in my machine and let me know.
If

We have sent a follow up to the **getgrav/grav** team. We will try again in 7 days. a year ago

A getgrav/grav maintainer a year ago

I followed your instructions (using git to install) and I'm still getting `Forbidden` for every file I try to access.

What happens if you click on 'Typography` menu item? If the page doesn't work, your server doesn't read the .htaccess file -> server configuration issue.

takester a year ago Researcher

Page is working --> "http://127.0.0.1:8000/typography"
Is it due to I am running "bin/grav install" as "sudo bin/grav install"

takester a year ago Researcher

and if I run only "bin/grav install" then the server is not running, means it is throwing error after entering "http://127.0.0.1:8000" (Even homepage is not getting load)

takester a year ago Researcher

***typo bin/grav install == bin/grav server

takester a year ago Researcher

Page is working --> "http://127.0.0.1:8000/typography"
Is it due to I am running "bin/grav server" as "sudo bin/grav server"

and if I run only "bin/grav server" then the server is not running, means it is throwing error after entering "http://127.0.0.1:8000" (Even homepage is not getting load)

Matias Griese validated this vulnerability a year ago

takester has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Matias Griese a year ago

OK, it looks like this is valid if using `bin/grav server`. That said, I think the documentation says it's only meant for development...

Nevertheless, I think it's good to have it to follow the same tules as Apache.

Matias Griese marked this as fixed with commit 8f9c41 a year ago

Matias Griese has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Jamie Slome a year ago Admin

CVE published! 🎊

takester a year ago Researcher

Thank you so much ✌️

Sign in to join this conversation