huntr

Authorization Bypass Through User-Controlled Key in weseek/growi

0

✓ Valid Reported on Sep 8th 2021

✍️ Description

In following endpoint don't check the authorization of users and any user can delete other users comments `/_api/comments.remove`
the body of request is like this :

```
{
"comment_id"  :  "61393bb36970d0000c62b3cf"


,

"_csrf"  : <a_new_one>

}
```

any user receive all `comment_id` and can easily replace other users `comment_id` with own `comment_id` and delete other user's comments.

💥 Impact

This vulnerability is capable of make high impact on integrity of system.

CVE
CVE-2021-3852
(Published)

Vulnerability Type
CWE-639: Authorization Bypass Through User-Controlled Key

Severity
Medium (6.3)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

amammad
@amammad
pro

This report was seen 417 times.

Z-Old a year ago Admin

Hey ammamad, I've emailed the maintainers for you.

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

A **weseek/growi** maintainer validated this vulnerability a year ago

amammad has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A **weseek/growi** maintainer a year ago Maintainer

We will fix it. Please wait the next release.

A **weseek/growi** maintainer marked this as fixed in **4.4.8** with commit **863bfd** a year ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Chat with us

A **weseek/growi** maintainer a year ago Maintainer

Thanks for reporting the vulnerability. It has already been fixed and released on v4.8.8.
Thank you.

Jamie Slome a year ago Admin

At the request of Kaori Tokashiki, we have gone ahead and assigned and published CVE-2021-3852.

If you have any further questions don't hesitate to get in touch.

A **weseek/growi** maintainer a year ago Maintainer

@admin
Hi, thanks for publishing the CVE.

By the way, e-mail automatic delivery system seems to be set to “vuls@jpcert.or.jp” which is different organization from GROWI project.
Could you replace it to “ml-jvn-growi@weseek.co.jp”?

A **weseek/growi** maintainer a year ago Maintainer

Sorry, I made a mistake on the comment 3 before. The released version is v4.4.8 not v4.8.8.

Jamie Slome a year ago Admin

@maintainer - you are welcome!

We can replace it, however, I attempted sending an e-mail to this new address yesterday, and it failed to deliver?

I will try another test e-mail now if that is okay.

Jamie Slome a year ago Admin

Just tried and I receive this error from our e-mail provider:

550 5.1.1 The email account that you tried to reach does not exist. Please try double-checking the recipient's email address for typos or unnecessary spaces.

A **weseek/growi** maintainer a year ago Maintainer

@admin
Could you try it again with "ml-jvn-growi@weseek.co.jp"?

A **weseek/growi** maintainer a year ago Maintainer

↑please ignore the comment.
@admin
Could you try it again with "ml-jvm-growi@weseek.co.jp"?

Jamie Slome a year ago Admin

It looks like that one was sent, can you confirm that you received this e-mail? After, we can go ahead and update the contact details for future notifications and reports.

A **weseek/growi** maintainer a year ago Maintainer

I replied to your email just now. Please check.

Jamie Slome a year ago Admin

I received it - shall I go ahead and update your contact address to this new e-mail?

Sign in to join this conversation