huntr

Cross-Site Request Forgery (CSRF) in area17/twill

✓ Valid Reported on Oct 27th 2021

0

Description

Attacker is able to logout a user if a logged in user visits attacker website.

Impact

This vulnerability is capable of forging user to unintentional logout.

Test

Tested on Edge, firefox, chrome and safari.

Fix

You should use POST instead of GET.

To expand:

One way GET could be abused here is that a person (competitor perhaps:) placed an image tag with src="<your logout link>" ANYWHERE on the internet, and if a user of your site stumbles upon that page, he will be unknowingly logged out.
This is why it should be a POST with a @csrf token.
While this cannot harm a users account it can be a great annoyance.

Occurrences

auth.php L8 _user.blade.php L17

CVE
CVE-2021-3932
(Published)

Vulnerability Type
CWE-352: Cross-Site Request Forgery (CSRF)

Severity
Medium (6.3)

Visibility
Public

Status
Fixed

Found by

HDVinnie
@hdvinnie
maintainer

Fixed by

Patrick Boivin
@pboivin
maintainer

This report was seen 409 times.

We have contacted a member of the **area17/twill** team and are waiting to hear back a year ago

We have sent a follow up to the **area17/twill** team. We will try again in 7 days. a year ago

Patrick Boivin validated this vulnerability a year ago

HDVinnie has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Patrick Boivin marked this as fixed with commit 81d80d a year ago

Patrick Boivin has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Chat with us

auth.php#L8 has been validated ✓

_user.blade.php#L17 has been validated ✓

Quentin Renard a year ago

@admin Hi there! I'm reaching out to ask if you can do anything to update the advisory that was created out of this report. Even though we have tagged a release with this fix, the GitHub advisory is still indicating that no patch is available: https://github.com/advisories/GHSA-f99g-pg48-wrfc. We are wondering if that is happening because we merged the fix under a different commit SHA.

Jamie Slome a year ago Admin

Hello, Quentin 👋 Thanks for getting in touch with your question.

I don't believe that this is something we can update from our side. I have just taken a look at all of the values that we can populate the CVE with, and the patched version is not its own field in the CVE meta.

Here is the method of publishing the CVE: LINK

Perhaps it has something to do with the `<= 2.5.2` we have provided in the CVE?

I would drop a message or e-mail to the GitHub Security Advisory team, and they should be able to shed some light on this issue.

Quentin Renard a year ago

Thanks for the speedy reply, Jamie. I just opened a ticket with GitHub Support.

Jamie Slome a year ago Admin

No worries, Quentin!

Feel free to keep me in the loop, and happy to help where possible!

Sign in to join this conversation