Cross-site Scripting (XSS) - DOM in karma-runner/karma

1

Valid Reported on Jan 8th 2022

Description

DOM-based XSS is a vulnerability in which the attacker can inject arbitrary javascript code in any DOM sink that supports dynamic code execution. In our case, `source` is query parameter `return_url` and sink is `location.href` .

Proof of Concept

1 Start karma server and visit the following link:

`http://localhost:9876/?return_url=javascript:alert(document.domain)`

Impact

The attacker can execute malicious javascript code in victim's browser like run crypto miners, exploit 0-day remote code execution bugs in browser etc.

CVE
CVE-2022-0437
(Published)

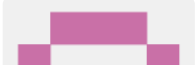
Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - DOM

Severity
Medium (5.4)

Visibility
Public

Status
Fixed

Found by



Rohan Sharma
@r0hansh

@rohansh

unranked

This report was seen 619 times.

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

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

We have contacted a member of the **karma-runner/karma** team and are waiting to hear back a year ago

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

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

A **karma-runner/karma** maintainer validated this vulnerability 10 months ago

Rohan Sharma has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Rohan Sharma 10 months ago Researcher

Hi,

I was about to fix the vulnerability after you validated it. But, it is really good that you fixed the bug yourself.

However, I have a doubt.
The current fix only allows `http` and `https` protocol in `return_url`. This will allow the people to exploit another vulnerability `Open Redirect` which means attacker can redirect people to other websites by having them visit `http://localhost:9876/?return_url=https://example.com`
Is this an acceptable risk? It will not be considered as a security vulnerability in the future? or we can plan to resolve that bug as well.

Rohan Sharma 10 months ago

@maintainer

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

A **karma-runner/karma** maintainer marked this as fixed in **6.3.14** with commit **839578**
10 months ago

The fix bounty has been dropped ✕

This vulnerability will not receive a CVE ✕

A **karma-runner/karma** maintainer 10 months ago Maintainer

I do not see how `Open Redirect` is a vulnerability. Please help me understand.

Rohan Sharma 10 months ago Researcher

`Open Redirect` is usually a low severity vulnerability. It's like people trust `example.com` and when they visit `example.com/?url=http://attacker.com`, they will get redirected to `attacker.com` where attacker might be running a 0-day browser exploit, crypto-miners and other malicious stuff which may cause any type of harm to a user.

Jonathan 10 months ago

What would be your approach to mitigate that vulnerability?

Rohan Sharma 10 months ago Researcher

Actually, I have not looked into the code for this redirect use-case.
In order to mitigate `Open Redirect` vuln, we should load trusted domains only like `subdomains of location`, `a set of trusted domains` etc.

Jonathan 10 months ago

I submitted https://github.com/karma-runner/karma/pull/3759 to mitigate that :)

Sign in to join this conversation