eclipse-theia / **theia** Public

Code | Issues 1.4k | Pull requests 26 | Discussions | Actions | ···

New issue

Jump to bottom

[security] XSS vulnerability in markdown preview #7954

Closed **caseyflynn-google** opened this issue on Jun 3, 2020 · 16 comments

Assignees

Labels security

caseyflynn-google commented on Jun 3, 2020 • edited ▾ Contributor

Bug Description: XSS vulnerability in markdown preview

The Markdown Preview can exploited to execute arbitrary code.

Steps to Reproduce:

1. Create markdown file and append the following text: <style onload="alert(0)">
2. Save and close the file.
3. Right click the file and select Open With -> Preview
4. Observe the alert has fired.

The root cause of the vulnerability is the current usage of markdown-it to render html then subsequently adding the output to the DOM via innerHtml without sanitizing. Moreover, there are several potential xss sinks within the Theia code base that could potentially be exploited in a similar fashion (e.g. innerHtml, dangerouslySetInnerHtml). Would the community be open to accepting contributions to mitigate these vulnerabilities, and accompanying lint rules that would bar future usages of xss sinks?

Additional Information

- Operating System: Linux
- Theia Version: 1.2.0

👀 1

caseyflynn-google added the **security** label on Jun 3, 2020

akosyakov commented on Jun 4, 2020 Member

> Would the community be open to accepting contributions to mitigate these vulnerabilities, and accompanying lint rules that would bar future usages of xss sinks?

I would be fine with it. **@marcdumais-work** @eclipse-theia/ecd-theia-committers any concerns?

👍 5

akosyakov commented on Jun 4, 2020 Member

I think the ideal solution would be to run any remote HTML content as webviews: #6562 And let them do whatever they want.

spoenemann mentioned this issue on Jun 4, 2020

Sanitize README content eclipse/openvsx#120

Closed

spoenemann commented on Jun 4, 2020 Contributor

Here's another piece of code where this problem is relevant:

theia/packages/vsx-registry/src/browser/vsx-extension.tsx
Line 385 in `c80f3fe`

```
385    dangerouslySetInnerHTML={{ __html: readme }} />}
```

thegecko commented on Jun 4, 2020 Member

> Would the community be open to accepting contributions to mitigate these vulnerabilities

I don't see any drawbacks, this would be great!

👍 1

jbicker self-assigned this on Jun 5, 2020

jbicker commented on Jun 5, 2020 Contributor

> Here's another piece of code where this problem is relevant:

theia/packages/vsx-registry/src/browser/vsx-extension.tsx
Line 385 in c80f3fe

```
385     dangerouslySetInnerHTML={{ __html: readme }} />}
```

This should be already solved here:
https://github.com/eclipse-theia/theia/blob/master/packages/vsx-registry/src/browser/vsx-extensions-model.ts#L208

👍 1

jbicker added a commit that referenced this issue on Jun 5, 2020

`Sanitizing markdown text.` ··· ✓ 973e208

jbicker mentioned this issue on Jun 5, 2020

Sanitizing markdown text. #7971

Merged

1 task

jbicker commented on Jun 5, 2020 Contributor

@caseyflynn-google I created a PR where I sanitize the md. However this does not contain any solutions regarding lint rules. Another PR for that is still welcome.

👍 1

jbicker added a commit that referenced this issue on Jun 8, 2020

`Sanitizing markdown text.` ··· ✓ e7e92e3

jbicker closed this as completed in `309b218` on Jun 8, 2020

akosyakov reopened this on Jun 8, 2020

akosyakov commented on Jun 8, 2020 Member

@caseyflynn-google Is anything else has to be done?

caseyflynn-google commented on Jun 9, 2020 • edited Contributor Author

Sorry for the delayed response, this looks great! I am digging into a few options for flagging usage of xss sinks via eslint rules. https://github.com/mozilla/eslint-plugin-no-unsanitized looks promising, but I will need to reach out to the owner to ensure they are willing to accept a contribution to enable running the rule over typescript: mozilla/eslint-plugin-no-unsanitized#111 (comment) It looks like the code is licensed under MPL-2.0 would that be a problem?

👍 1

akosyakov commented on Jun 10, 2020 Member

> It looks like the code is licensed under MPL-2.0 would that be a problem?

@marcdumais-work ? fyi we will use it only as a dev dependency.

marcdumais-work commented on Jun 10, 2020 • edited Contributor

> @marcdumais-work ? fyi we will use it only as a dev dependency.

MPL-1.1/MPL-2.0 (Mozilla Public License) is fine even as runtime dependency, being part of the Eclipse Foundation approved license list

jbicker removed their assignment on Jun 10, 2020

caseyflynn-google self-assigned this on Jun 10, 2020

akosyakov mentioned this issue on Aug 17, 2020

Is Theia interested in expanding their ESLint config to include XSS sink scanning #8398

Closed

JLLeitschuh commented on Nov 10, 2020

Has this had a CVE assigned to it?

👀 1

luigigubello mentioned this issue on Nov 28, 2020

Adding a security policy to the repo #8795

Closed

luigigubello mentioned this issue on Dec 16, 2020

Add SECURITY.md #8842

Closed

1 task

AdamGold commented on Feb 16, 2021 • edited

Hey, Adam from Snyk here. Would you like us to issue a CVE for this?

waynebeaton commented on Feb 22, 2021

The Eclipse Foundation is a CNA can assign a CVE at the project team's request. Specifically, the request needs to be initiated by a committer.

We need the project team to provide some information; this is described in the handbook.

marcdumais-work commented on Feb 24, 2021 • edited Contributor

Hi,

Sorry for the delay. Here it is:

Description: In Eclipse Theia versions up to and including 1.2.0, the Markdown Preview (@theia/preview), can be exploited to execute arbitrary code.
Categorization: CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
Versions: 0 to 1.2
This vulnerability has been patched in Eclipse Theia v1.3.0

(PR: #7971)

👍 1

waynebeaton commented on Feb 24, 2021

Thanks, **@marcdumais-work**.

I've assigned CVE-2020-27224. I've pushed the report and it has been merged, it should go live shortly.

👍 2

marcdumais-work commented on Feb 24, 2021 Contributor

Thanks Wayne. I think we can close this issue.

marcdumais-work closed this as completed on Feb 24, 2021

Assignees

caseyflynn-google

Labels

security

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

9 participants