eclipse-theia / theia Public

<> Code ⊙ Issues 1.4k Pull requests 25 Discussions Actions ···

New issue

Jump to bottom

Javascript injection via notification messages #7283

Closed luigigubello opened this issue on Mar 5, 2020 · 5 comments · Fixed by #7289

Assignees

Labels help wanted notifications security

luigigubello commented on Mar 5, 2020

Description

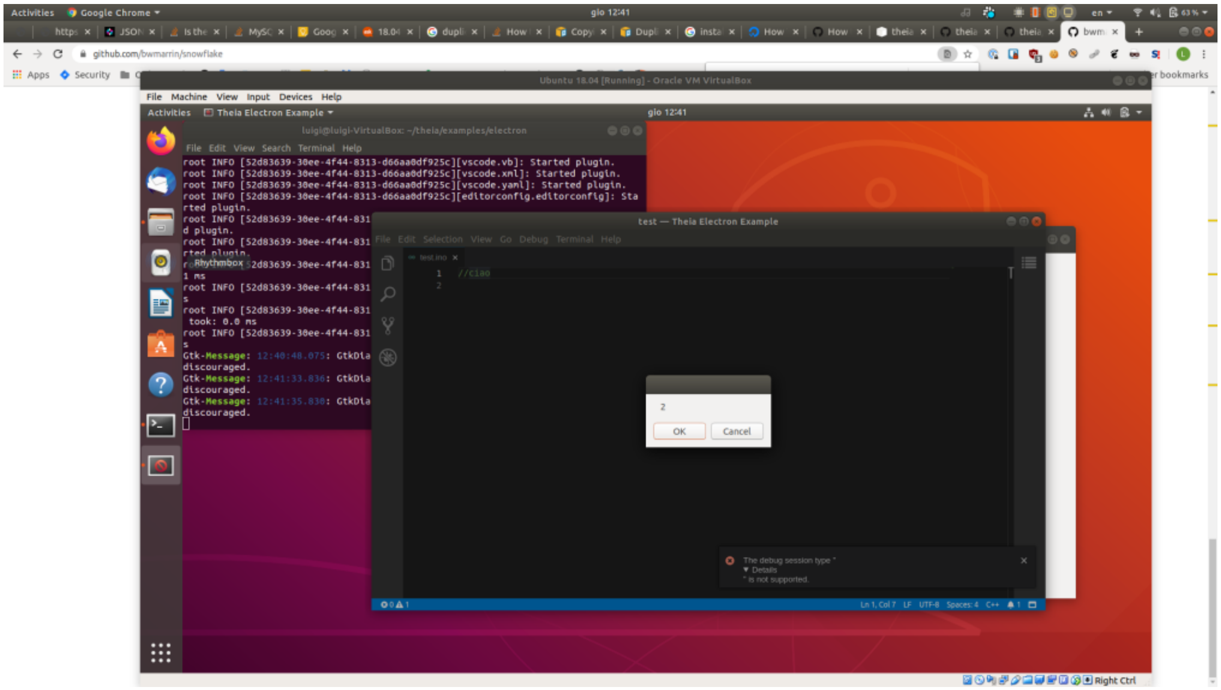
In the notification messages there is no an HTML escaping, so Javascript code can run. I'm not sure, but I think the issue is in packages/messages/src/browser/notification-component.tsx:76

```
<span dangerouslySetInnerHTML={{ __html: message }} onClick={this.onMessageClick} />
```

In Electron app an arbitrary JS code can lead to dangerous exploits.

Reproduction Steps

- Create a new project and create a new debugger configuration file `launch.json`
- In the `type` field write the Javascript payload (e.g. `<details open ontoggle=confirm(2)>`)
- Press F5 to launch the debugger and see the alert box



Activities
Google Chrome
gio 12:41
github.com/bwmarrin/snowflake
Apps
Security
bookmarks
Ubuntu 18.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Theia Electron Example
gio 12:41
luigi@luigi-VirtualBox: ~/theia/examples/electron
File Edit View Search Terminal Help
Rhythmbox
test — Theia Electron Example
File Edit Selection View Go Debug Terminal Help
test.ino
OK
Cancel
Ln 1, Col 7 LF UTF-8 Spaces: 4 C++ 1
Right Ctrl

```
root INFO [52d83639-30ee-4f44-8313-d66aa0df925c][vscode.vb]: Started plugin.
root INFO [52d83639-30ee-4f44-8313-d66aa0df925c][vscode.xml]: Started plugin.
root INFO [52d83639-30ee-4f44-8313-d66aa0df925c][vscode.yaml]: Started plugin.
root INFO [52d83639-30ee-4f44-8313-d66aa0df925c][editorconfig.editorconfig]: Sta
rted plugin.
root INFO [52d83639-30ee-4f44-831
d plugin.
root INFO [52d83639-30ee-4f44-831
rted plugin.
r                  52d83639-30ee-4f44-831
1 ms
root INFO [52d83639-30ee-4f44-831
s
root INFO [52d83639-30ee-4f44-831
 took: 0.0 ms
root INFO [52d83639-30ee-4f44-831
s
Gtk-Message: 12:40:48.075: GtkDia
discouraged.
Gtk-Message: 12:41:33.836: GtkDia
discouraged.
Gtk-Message: 12:41:35.830: GtkDia
discouraged.
```

```
1  //ciao
2
```

2

The debug session type "
▼ Details
" is not supported.

OS and Theia version:

- Ubuntu 18.04
- Theia Electron Example 0.16.0

I think this bug is a vulnerability, I can exfiltrate data from victim's computer by using JS. Here a proof-of-concept video.

Theia_PoC.zip

👍 1 🚀 1

kittaakos added the security label on Mar 5, 2020

akosyakov added help wanted notifications labels on Mar 5, 2020

akosyakov commented on Mar 5, 2020 Member

cc @AlexTugarev

akosyakov commented on Mar 5, 2020 Member

> I think this bug is a vulnerability, I can exfiltrate data from victim's computer by using JS.

Extensions already have access to all operating systems APIs. There is no need to inject JS in the notification center 😝

I think we should fix it anyway.

> In Electron app an arbitrary JS code can lead to dangerous exploits.

In order to be completely safe, we need to enable web security in electron and run remote content like mini browser as webviews, otherwise any loaded JS code can user Node.js API to access everything directly.

spoenemann commented on Mar 6, 2020 Contributor

While we're changing the way we render notifications, can we make sure that line breaks in the notification text are displayed as such? I already found myself "using" this exploit in the past by replacing `\n` with `<br/>` before submitting a notification message.

AlexTugarev self-assigned this on Mar 6, 2020

AlexTugarev commented on Mar 6, 2020 • edited Contributor

Will align with vscode for that matter.

@spoenemann, that's not supported, cf. https://github.com/Microsoft/vscode/blob/5651fa0a8a482ba8427797ba2c053b1943ff15fb/src/vs/workbench/common/notifications.ts#L493

😕 1

AlexTugarev mentioned this issue on Mar 6, 2020

[notifications] disallow arbitrary html in message content #7289

Merged

1 task

AlexTugarev closed this as completed in #7289 on Mar 9, 2020

vince-fugnitto mentioned this issue on Mar 12, 2020

VSCodeAPI 'showInformationMessage' do not support newlines. (\n) #7332

Closed

kittaakos mentioned this issue on Jun 23, 2020

Modal notification does not render newlines or have a max-width #8071

Closed

This was referenced on Nov 28, 2020

XSS in Debug Console [Theia v1.8.0] #8794

Closed

Adding a security policy to the repo #8795

Closed

luigigubello mentioned this issue on Dec 16, 2020

Add SECURITY.md #8842

Closed

1 task

waynebeaton commented on Mar 12, 2021

I've assigned CVE-2021-28162 with this description:

> In Eclipse Theia versions up to and including 0.16.0, in the notification messages there is no HTML escaping, so Javascript code can run.
>
> CWE-830: Inclusion of Web Functionality from an Untrusted Source

Let me know if updates are required.

Assignees

AlexTugarev

Labels

help wanted notifications security

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

[notifications] disallow arbitrary html in message content
eclipse-theia/theia

6 participants