New issue

Jump to bottom

Potential command execution vulnerability introduced by unsafe IPC exposure #142

Closed xiaofen9 opened this issue on Mar 9, 2021 · 3 comments

Assignees

xiaofen9 commented on Mar 9, 2021

Hi,

Great work!
We did a security analysis on the app and found that the risky `ipcRenderer` is directly exposed to the unsafe renderer process. This may allow remote attackers to abuse sensitive methods in the (privileged) main process by crafting malicious IPC messages.

Vulnerability Details

The following code shows how a preload script exposes IPC.

twinkle-tray/src/intro-preload.js
Line 39 in 16c4a71

```
39    window.ipc = ipc
```

We do find exploitable IPC endpoints. e.g.,
If the attacker sends a malicious msg to `open-url` channel, he may execute arbitrary commands via `openExternal`.

twinkle-tray/src/electron.js
Lines 1314 to 1316 in 3871712

```
1314    ipcMain.on('open-url', (event, url) => {
1315      require("electron").shell.openExternal(url)
1316    })
```

Mitigation

- enforce security checks when receiving events on sensitive channels (e.g., check if received URL is legal before openExternal)
- avoid directly exposing ipcRenderer to untrusted domains.

xanderfrangos commented on Mar 9, 2021 Owner

Thanks for the security audit. 👍 I'll get this patched up.

xanderfrangos self-assigned this on Mar 9, 2021

xanderfrangos added a commit that referenced this issue on Mar 9, 2021

`Use pre-defined list for 'open-url' IPC` ... `643633f`

abergmann commented on Mar 10, 2021

CVE-2021-28119 was assigned to this issue.

xanderfrangos commented on Mar 25, 2021 Owner

v1.13.4 has been released with a fix for this potential vulnerability. I now use a pre-defined list of URLs.

I am not aware of any way that IPC could be triggered from outside of Electron, and Twinkle Tray does not load any HTML/JS from external URLs (it's all contained in the distributed ASAR). But just in case it *is* possible to exploit, it's been fixed. Thanks again for pointing the vulnerability out.

xanderfrangos closed this as completed on Apr 5, 2021

Assignees
xanderfrangos

Labels
None yet

Projects
None yet

Milestone
No milestone

Development

No branches or pull requests

3 participants