popcorn-official / popcorn-desktop Public

Code Issues 23 Pull requests 2 Actions Projects 1 Wiki •••

New issue Jump to bottom

Popcorn Time 0.4.7 - XSS to RCE #2491

Closed alestorm980 opened this issue on Apr 26 · 0 comments · Fixed by #2495

Labels bug

alestorm980 commented on Apr 26

Our security team found a security issue inside Popcorn Time 0.4.7. We have reserved the CVE-2022-25229 to refer to this issue. Attached below is the link to our responsible disclosure policy.

https://fluidattacks.com/advisories/policy

Bug description

Popcorn Time **0.4.7** has a Stored XSS in the `Movies API Server(s)` field via the `settings` page. The `nodeIntegration` configuration is set to **on** which allows the webpage to use `NodeJs` features, an attacker can leverage this to run OS commands.

CVSSv3 Vector:

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N

CVSSv3 Base Score:

7.7

Steps to reproduce

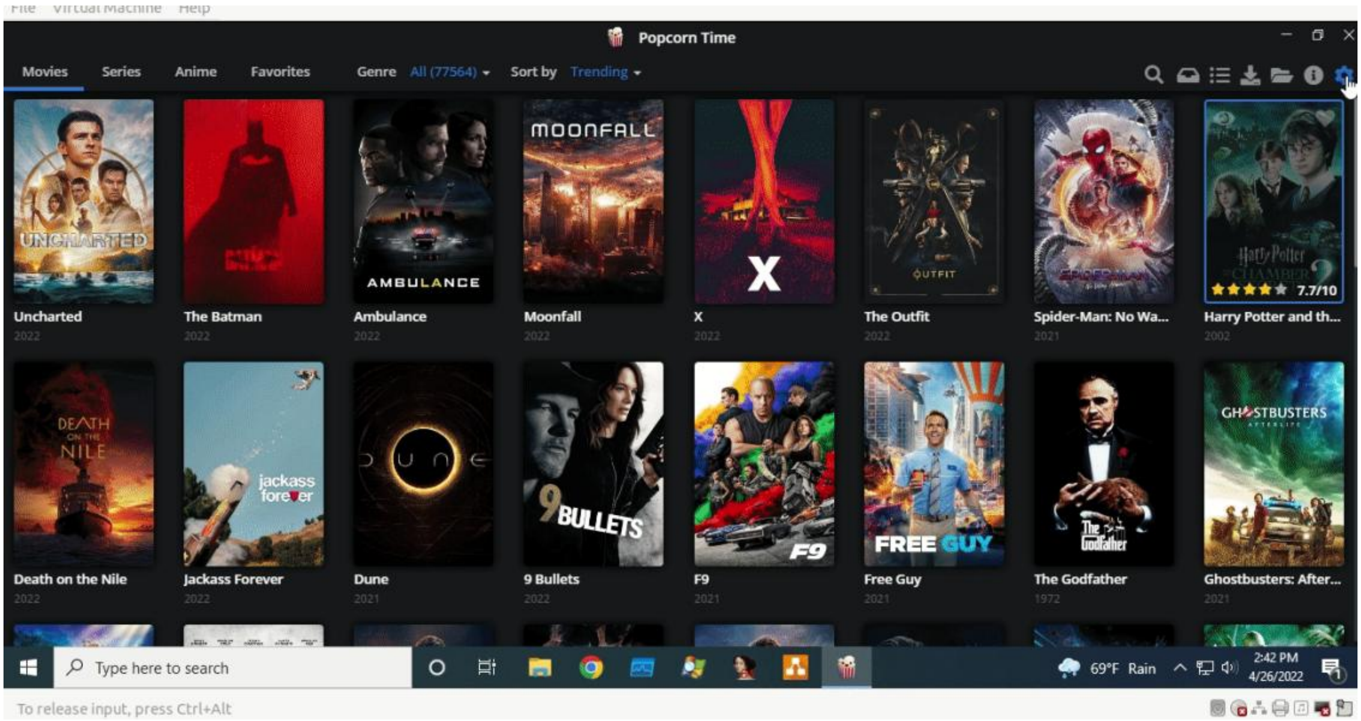
1. Open the Popcorn time application.
2. Go to `settings`.
3. Enable `Show advanced settings`.

4. Scroll down to the `API Server(s)` section.
5. Insert the following PoC inside the `Movies API Server(s)` field and click on `Check for updates`.

```
a"><script>require('child_process').exec('calc');</script>
```

6. Scroll down to the `Database` section and click on `Export database`.
7. The application will create a `.zip` file with the current configuration.
8. Send the configuration to the victim.
9. The victim must go to `Settings -> Database` and click on `Import Database`
10. When the victim restarts the application the XSS will be triggered and will run the `calc` command.

Screenshots and files



System Information

- Version: Popcorn Time 0.4.7.
- Operating System: Windows 10.0.19042 N/A Build 19042.
- Installer: Popcorn-Time-0.4.7-win64-Setup.exe

kiriles90 added this to **Verifying** in **Popcorn Time Desktop** via automation on Apr 30 kiriles90 added the bug label on May 4

kiriles90 moved this from **Verifying** to **Bugs** in **Popcorn Time Desktop** on May 4

kiriles90 mentioned this issue on May 7

Fix XSS to RCE issue #2495

Merged

kiriles90 closed this as completed in #2495 on May 7

kiriles90 removed this from **Bugs** in **Popcorn Time Desktop** on May 7

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Fix XSS to RCE issue

2 participants