Home / Advisories / Popcorn Time 0.4.7 XSS to RCE

Popcorn Time 0.4.7 - XSS to RCE

Summary

Name	Popcorn Time 0.4.7 - XSS to RCE

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

State	Public
Release date	2022-05-17

Vulnerability

Kind	XSS to RCE
Rule	010. Stored cross-site scripting (XSS)
Remote	No
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
Exploit available	No
CVE ID(s)	CVE-2022-25229

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Proof of Concept

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.

System Information

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

There is no exploit for the vulnerability but can be manually exploited.

Mitigation

An updated version of PopcornTime is available at the vendor page.

Credits

The vulnerability was discovered by Oscar Uribe from the Offensive Team of `Fluid Attacks`.

References

Vendor page https://github.com/popcorn-official/popcorn-desktop

Issue https://github.com/popcorn-official/popcorn-desktop/issues/2491

Timeline

- 2022-04-26
  Vulnerability discovered.
- 2022-04-26
  Vendor contacted.
- 2022-05-04
  Vendor Confirmed the vulnerability.
- 2022-05-07
  Vulnerability patched.
- 2022-05-17

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Services

Continuous Hacking

One-shot Hacking

Comparative

Solutions

DevSecOps

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Advisories

FAQ

Documentation

Contact

Copyright © 2022 Fluid Attacks. We hack your software. All rights reserved.

Service Status - Terms of Use - Privacy Policy - Cookie Policy