apexcharts / **apexcharts.js** Public

Code | Issues 220 | **Pull requests** 3 | Discussions | Actions | Projects | ···

New issue

Jump to bottom

Security Fix for Cross-Site Scripting (XSS) - huntr.dev #2158

Merged **junedchhipa** merged 2 commits into `apexcharts:master` from `418sec:1-npm-apexcharts` on Jan 14, 2021

Conversation 3 | Commits 2 | Checks 0 | Files changed 3

huntr-helper commented on Jan 14, 2021

https://huntr.dev/users/arjunshibu has fixed the Cross-Site Scripting (XSS) vulnerability 🔨. Think you could fix a vulnerability like this?

Get involved at https://huntr.dev/

Q | A
Version Affected | ALL
Bug Fix | YES
Original Pull Request | 418sec#1
Vulnerability README | https://github.com/418sec/huntr/blob/master/bounties/npm/apexcharts/1/README.md

User Comments:

📊 Metadata *

Bounty URL: https://www.huntr.dev/bounties/1-npm-apexcharts

⚙️ Description *

`apexcharts` is vulnerable to Cross-Site Scripting (XSS).

💻 Technical Description *

The package does not properly validate some chart fields. This causes `XSS` and the payload is triggered when `tooltip` and `label` fields are rendered. The fix is implemented by sanitizing those fields before rendering them.

🐛 Proof of Concept (PoC) *

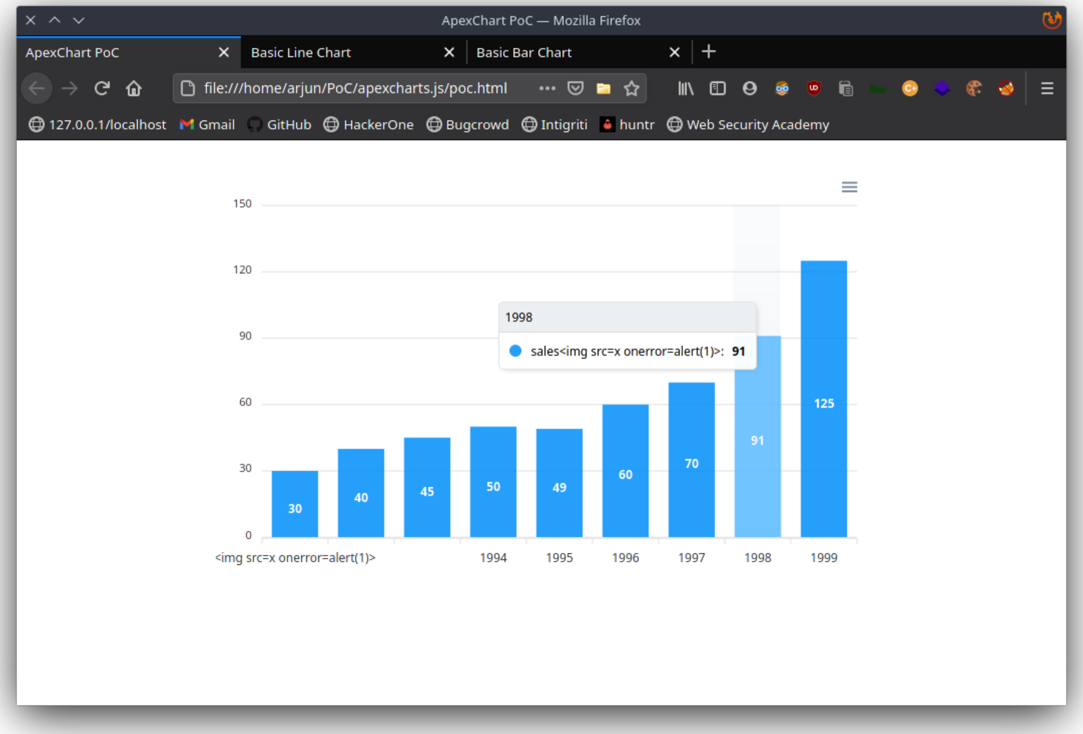
1. Install the package by following this instruction https://apexcharts.com/docs/installation/ or try the live sandbox here https://codepen.io/apexcharts/pen/xYqyYm
2. Edit `JS` and insert the XSS payload below in the `name` field
3. Payload: `'sales<img src=x onerror=alert(1)>'`
4. XSS payload will get executed.

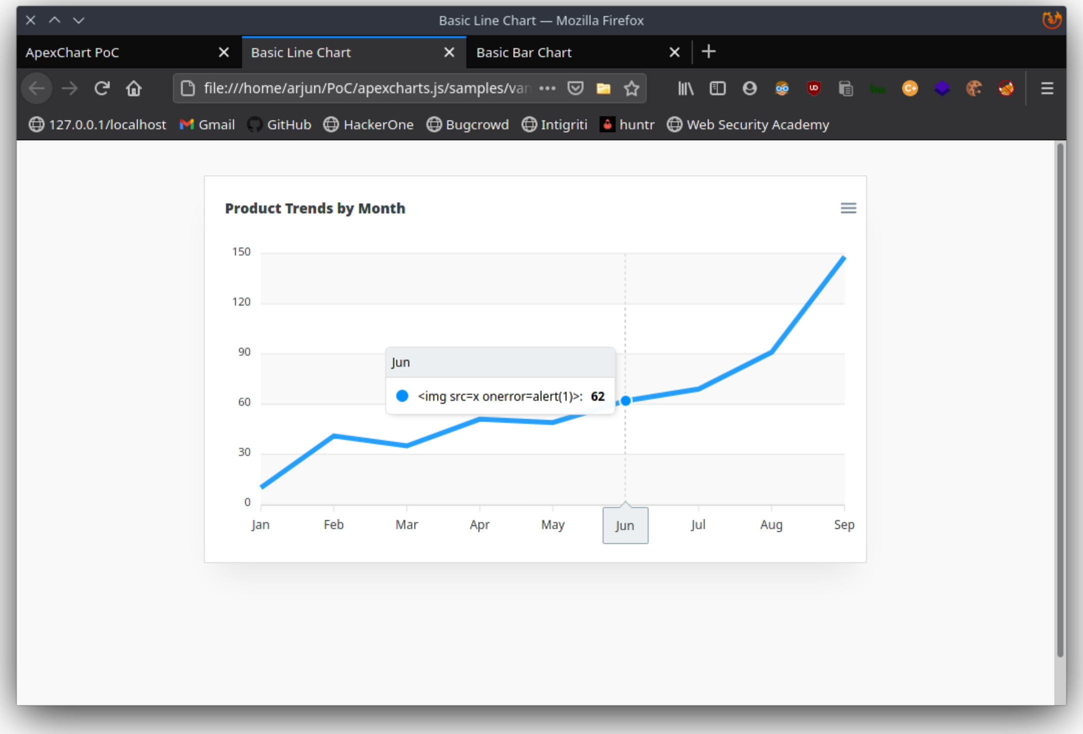
🔥 Proof of Fix (PoF) *

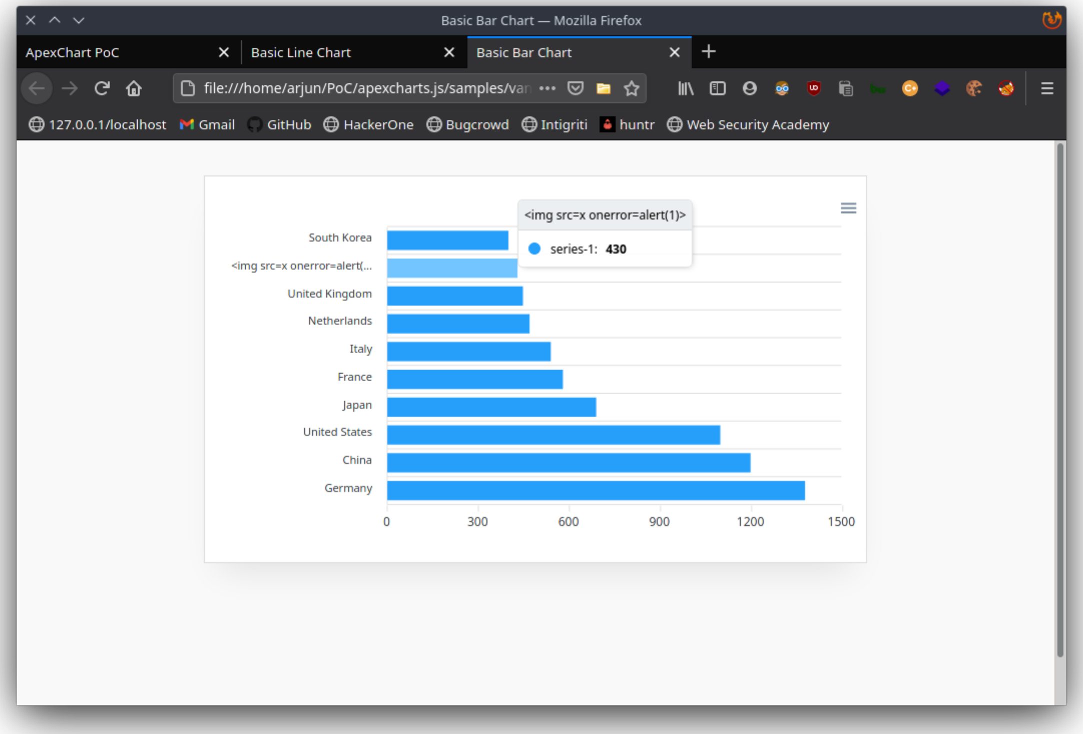
Build package to apply fix

```
npm run dev
# or
npm run build
```

XSS is fixed as shown below.







+1 User Acceptance Testing (UAT)

- I've executed unit tests.
- After fix the functionality is unaffected.

arjunshibu and others added 2 commits 2 years ago

```
Security fix for Cross-Site Scripting in apexcharts                9a7425c
Merge pull request #1 from arjunshibu/master  …                    e4c30a4
```

JamieSlome commented on Jan 14, 2021 Contributor

@junedchhipa - let me know if you have any questions or thoughts, cheers! 🍰

junedchhipa approved these changes on Jan 14, 2021

View changes

junedchhipa merged commit **68f3f34** into `apexcharts:master` on Jan 14, 2021

junedchhipa commented on Jan 14, 2021 Contributor

Thank you for your contribution!

❤️ 2 🚀 2

JamieSlome commented on Feb 21, 2021 Contributor

@junedchhipa, if you want more security fixes and patches like this in the future, you can let security researchers know that they can win bounties protecting your repository by copying this small code snippet into your README.md:

```
[![huntr](https://cdn.huntr.dev/huntr_security_badge_mono.svg)](https://huntr.dev)
```

👇 👇 👇

security bounty | up to $750 + CVE

Reviewers

junedchhipa ✓

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

4 participants