15

Reflected XSS in the npm module express-cart.

Share:

TIMELINE

avi3719 submitted a report to Node.js third-party modules. Aug 16th (4 years ago)

> NOTE! Thanks for submitting a report! Please replace *all* the [square] sections below with the pertinent details. Remember, the more detail you provide, the easier it is for us to triage and respond quickly, so be sure to take your time filling out the report!

I would like to report Reflected XSS in the npm module express-cart.
It allows a user to insert malicious payload in the user input field and the script gets reflected in the browser

Module

module name: express-cart
version: 1.1.5
npm page: `https://www.npmjs.com/package/express-cart`

Module Description

expressCart is a fully functional shopping cart built in Node.js (Express, MongoDB) with Stripe, PayPal, and Authorize.net payments.

Module Stats

[27] downloads in the last week

Vulnerability

Vulnerability Description

when the admin user creates a request for a new product, then the field 'Product option' accepts any malicious user input. This lead me to identify the reflected XSS attack.

Steps To Reproduce:

1. Login with admin user credentials.
2. From Left Menu panel, select new under product tab
3. In 'product options' details, insert any javascript payload eg. `<script>` alert(1234) `</script>`
4. The reflected XSS in the form of an alert box will be pop up in a browser window.

Supporting Material/References:

- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

> I technical information about the stack where the vulnerability was found

- OS used Windows 10
- NODEJS VERSION - V8.11.3
- NPM VERSION - 5.6.0
- Browser - Chrome 68.0.3440.106

Wrap up

- I contacted the maintainer to let them know: [N]
- I opened an issue in the related repository: [N]

Impact

This vulnerability would allow a user to insert javascript payloads which can be reflected in a browser.

2 attachments:
F334152: 2.png
F334153: 1.png