


[CVE-2020-15109] Ability to change order address without triggering address validations

Moderate kennyadsl published GHSA-3mvg-rrrw-m7ph on Jul 31, 2020

Package

 solidus_frontend, solidus_api (RubyGems)

Affected versions

< 2.10.2, < 2.9.6, < 2.8.6

Patched versions

2.10.2, 2.9.6, 2.8.6

Description

Impact

This vulnerability allows a malicious customer to craft request data with parameters that allow changing the address of the current order without changing the shipment costs associated with the new shipment.

All stores with at least two shipping zones and different costs of shipment per zone are impacted.

E.g.

1. Store admin configured the store so that there are two zones in US:

- East Cost Zone - Shipping Method cost: \$1
- West Cost Zone - Shipping Method cost: \$10

The attacker user can know that shipping to NY is less expensive than to LA just by testing different addresses in checkout.

2. The attacker user enters any NY shipping address in the address step
3. The attacker user chooses the \$1 delivery option
4. The attacker user crafts a request with their real LA address, similar to:

```
// POST #checkout/update:

{
  state: 'payment',
  order: {
    ship_address_attributes: {
      city: 'Los Angeles',
      ...
    }
  }
}
```

5. The attacker user proceeds with checking out with a new address and the \$1 shipment costs.

Another scenario where this could be dangerous is:

You cannot ship products in some zones and you are relying on Solidus Shipping Method building only to filter out unwanted zones. Malicious users can enter an allowed zone's address and change back to an unwanted one in the payment step by crafting a request with some proper ship_address_attributes.

This problem comes from how checkout permitted attributes are structured. We have a single list of attributes that are permitted across the whole checkout, no matter the step that is being submitted.

Patches

A PR has been attached to fix the security concern for each of all the Solidus supported versions following the rules of the [Solidus Security Policy](#).

Workarounds

When it's not possible to upgrade to a supported patched version, please use this gist to patch the store:

<https://gist.github.com/kennyadsl/4618cd9797984cb64f7700a81bda889d>

TODO

- ☒ Wait reviews on the PR proposed
- ☒ Backport to all other supported versions
- ☒ Create a workaround for who cannot update <https://gist.github.com/kennyadsl/4618cd9797984cb64f7700a81bda889d>
- ☒ Set a publishing date: **July, 16th**
- ☒ Write blogpost/newsletter/twitter/linkedin message (see previous [newsletter](#), [blogpost](#))
- ☒ Write a message to Spree/SparkSolution to let them know
- ☒ Request CVE to GH here
- ☐ Publish Advisory
- ☐ Release patched versions

Severity

Moderate

CVE ID

Weaknesses

No CWEs

Credits



[mamhoff](#)



[kennyadsl](#)