matestack / **matestack-ui-core** Public

Code · Issues 10 · Pull requests 28 · Actions · **Security 1** · Insights

XSS/Script injection vulnerability

High **jonasjabari** published **GHSA-3jqw-vv45-mjhh** on Feb 12, 2020

Package

No package listed

Affected versions	Patched versions
<= 0.7.3	>= 0.7.4

Description

Impact

- matestack-ui-core is vulnerable to XSS/Script injection
- matestack-ui-core does not excape strings by default and does not cover this in the docs
- matestack-ui-core should escape strings by default in order to prevent XSS/Script injection vulnerability

```
class Pages::MyApp::MyExamplePage < Matestack::Ui::Page

  class FakeUser < Struct.new(:name)
  end

  def prepare
    @user = FakeUser.new("<script>alert('such hack many wow')</script>")
  end

  def response
    components {
      div do
        heading size: 1, text: "Hello #{@user.name}" # is not escaped
        plain "Hello #{@user.name}" # is not escaped
      end
    }
  end
end
```

Patches

patched in 0.7.4

Workarounds

escape string explicitly/manually

References

reported by **@PragTob**

For more information

If you have any questions or comments about this advisory:

- Open an issue in matestack-ui-core
- Email us at jonas@matestack.io

Severity

High

CVE ID

CVE-2020-5241

Weaknesses

No CWEs

Credits

PragTob