Store XSS in title parameter executing at EditUser Page & EditProducto page in neorazorx/facturascripts

0

Valid Reported on Apr 20th 2022

Description

Cross-site scripting (XSS) is a common attack vector that injects malicious code into a vulnerable web application. Stored XSS, also known as persistent XSS, is the more damaging of the two. It occurs when a malicious script is injected directly into a vulnerable web application.

Proof of Concept

Login as Normal user.
Click on Options and select user.
Set title as <script>alert(document.domain)</script> and save. It will store the XSS payload.
log in to any account, i.e. admin.
Click on the top right corner i.e EditUser executing xss.

Video PoC

EditUser- https://drive.google.com/file/d/1zHI5GNU7JFUL5h6e64tnUFg4lXzqECRU/view?usp=sharing EditProducto- https://drive.google.com/file/d/1Z2fcc6DF-4eFpB1DAok3XMrtjUtYWo5M/view?usp=sharing

Impact

Cross-site scripting attacks can have devastating consequences. Code injected into a vulnerable application can exfiltrate data or install malware on the user's machine. Attackers can masquerade as authorized users via session cookies, allowing them to perform any action allowed by the user account.

References

- https://owasp.org/www-community/attacks/xss/

CVE
CVE-2022-1457

(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Critical (9)

Registry
Other

Affected Version
2021.81

Visibility
Public

Status
Fixed

Found by

Tarun Garg
@iamshooter99
pro

This report was seen 693 times.

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

Tarun Garg modified the report 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

Tarun Garg has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Carlos Garcia marked this as fixed in 2022.04 with commit b3e752 7 months ago

The fix bounty has been dropped ✕

This vulnerability will not receive a CVE ✕

Tarun Garg 7 months ago Researcher

Thank you for the reward, is there any CVE number that will also be assigned?

Tarun Garg 7 months ago Researcher

@neorazorx @admin Please check if CVE can be assigned

Jamie Slome 7 months ago Admin

Sure, we can assign a CVE here, we first require the go-ahead from the maintainer.

@maintainer - are you happy for us to assign and publish a CVE for this report?

Tarun Garg 7 months ago Researcher

@maintainer

Tarun Garg 7 months ago Researcher

@admin

Tarun Garg 7 months ago Researcher

@admin @maintainer, as the fix is already released, can you assign a CVE here

Jamie Slome 7 months ago Admin

Sorted 👍

Tarun Garg 7 months ago Researcher

Thank you

Sign in to join this conversation