huntr

Reflected Xss using url based payload in neorazorx/facturascripts

0

✓ Valid Reported on May 8th 2022

Description

Hi there i found that url parameter is not verified by server so an attacker can use javascript schema to run xss on user's browser

Proof of Concept

Visit this page http://localhost/invoices/EditPageOption?code=ListProducto-new&url=javascript:prompt(2)
Click on back button
PoC:-
https://youtu.be/I1uHfNa2p58

Impact

Xss can use to steal user's cookies which lead to Account takeover or do any malicious activity in victim's browser

CVE
CVE-2022-1682
(Published)

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

Severity
Critical (9.4)

Registry
Other

Affected Version
2022.06

2022.06

Visibility

Public

Status

Fixed

Found by

Distorted_Hacker

@gaurav-g2

pro

Fixed by

Carlos Garcia

@neorazorx

unranked

This report was seen 500 times.

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

Distorted_Hacker modified the report 7 months ago

Distorted_Hacker 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

Distorted_Hacker has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Carlos Garcia marked this as fixed in **2022.07** with commit **8e31d8** 7 month

Chat with us

Carlos Garcia has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Distorted_Hacker 7 months ago

Researcher

@admin can you assign cve ?

Jamie Slome 6 months ago

Admin

Sorted 👍

> Sign in to join this conversation