Stored XSS via upload plugin functionality in zip format in neorazorx/facturascripts

0

Valid Reported on Apr 21st 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. Here name parameter is vulnerable to xss. So after replacing the name with the XSS payload in the facturascripts.ini file. XSS payload will be executed after uploading the modified zip file.

Proof of Concept

log in as a Normal User.
Download any facturascripts plugin like (https://facturascripts.com/DownloadBuild/93/stable).
Unzip it locally and modify name = '<script>alert(document.domain)</script>' in facturascripts.ini file.
Zip it again and upload.
XSS payload will be executed for all users.

PoC

https://drive.google.com/file/d/18NGs-gTbwJVDB9P_1NCfQGUbjT1Jv9MC/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-2022-1514
(Published)

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

Severity
Critical (9)

Registry
Other

Affected Version
v2021.81

Visibility
Public

Status
Fixed

Found by

Tarun Garg
@iamshooter99
pro

This report was seen 713 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

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Tarun Garg 7 months ago Researcher

@maintainer @admin, thanks for the bounty, please assign a CVE for that.

Jamie Slome 7 months ago Admin

Before we assign and publish a CVE, we will first wait for the maintainer to confirm a fix against the report 👍

We have sent a fix follow up to the **neorazorx/facturascripts** team. We will try again in 7 days.
7 months ago

Tarun Garg 7 months ago Researcher

@maintainer

Carlos Garcia marked this as fixed in 2022.06 with commit aa9f28 7 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Tarun Garg 7 months ago Researcher

@admin @neorazorx @maintainer as the fix is also released please assign a CVE for this vulnerability.

Jamie Slome 7 months ago Admin

Sorted 👍

Sign in to join this conversation