Multiple Store XSS via upload svg file and the file name of attachment in neorazorx/facturascripts

0

Valid Reported on Apr 27th 2022

Description

Hi There, facturascripts is vulnerable to store XSS by upload svg file, and the filename

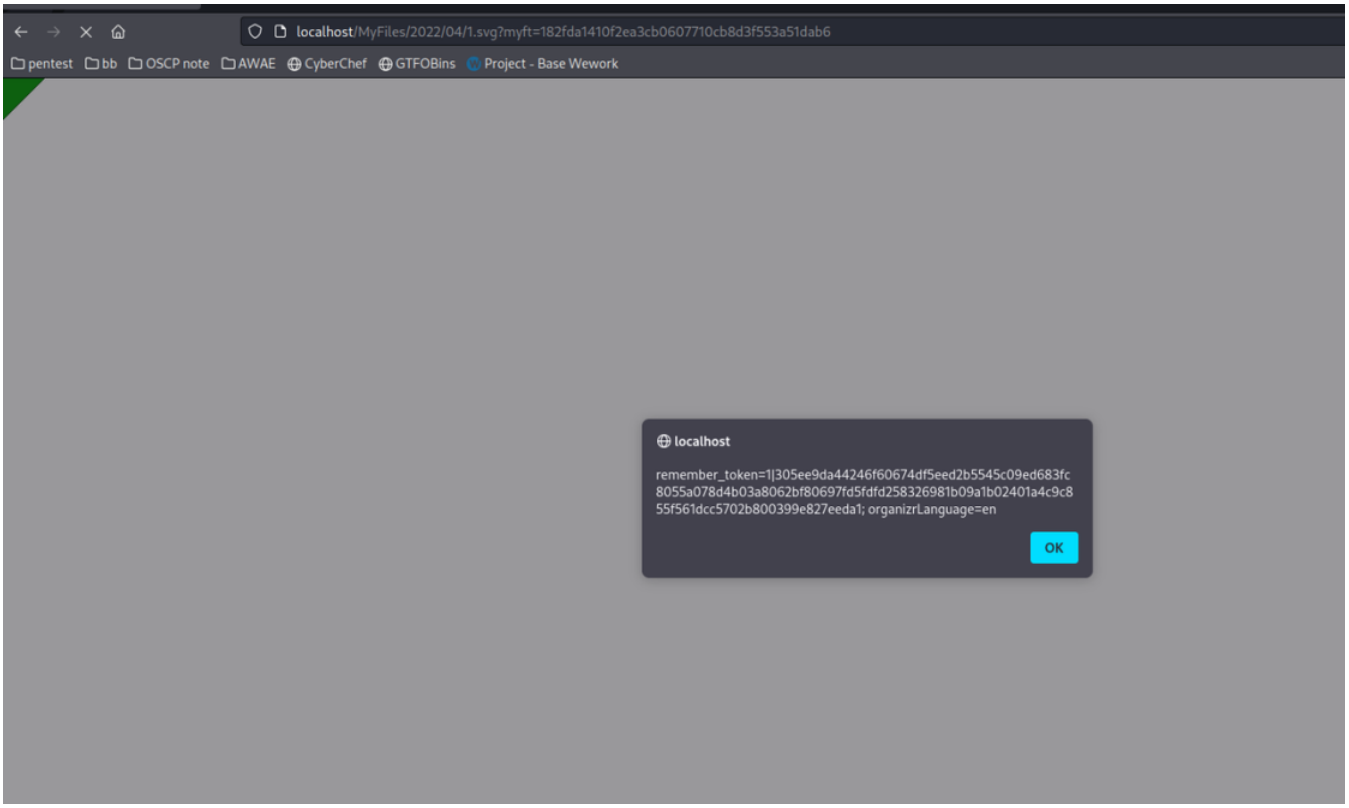
Step to produce with svg file

Login as admin or any account has role Admin->Library, access Admin -> library -> New and upload file svg with content:

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/

<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
   <polygon id="triangle" points="0,0 0,50 50,0" fill="#009900" stroke="#00
   <script type="text/javascript">
      alert(document.cookie);
   </script>
</svg>
```

save this. XSS will be trigger when you download it.



Step to produce with file name payload:

just upload file with the file name: `%22><img src=x onerror=alert(document.cookie).xlsx` -> xss will be 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 of the user's device.

CVE
CVE-2022-2065
(Published)

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

Severity
High (8.6)

Registry

Registry
Other

Affected Version

2021.81

Visibility
Public

Status
Fixed

Found by

Minh
@minhnb11
pro

This report was seen 663 times.

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

Minh modified the report 7 months ago

Minh 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

Minh has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

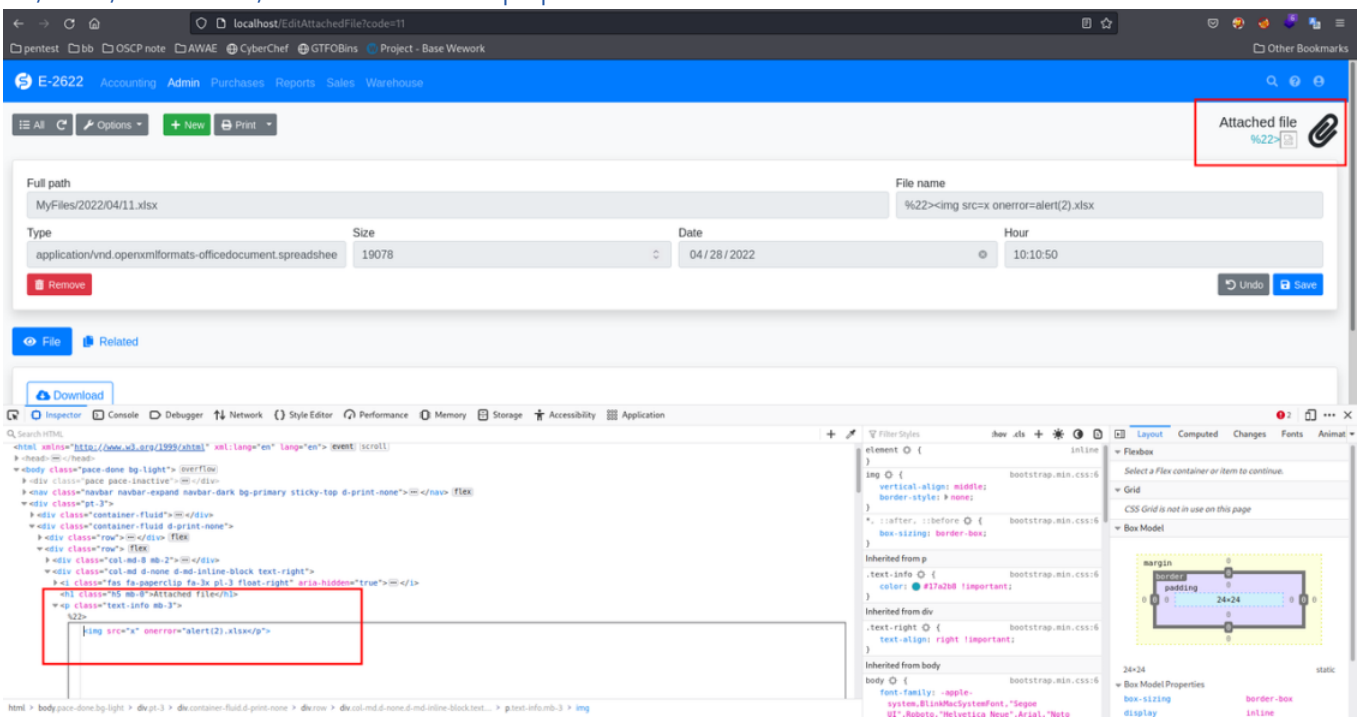
Carlos Garcia marked this as fixed in **2022.06** with commit **1d1edb** 7 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Minh 7 months ago Researcher

@neorazorx seem the xss on file name has not been fixed.
https://github.com/NeoRazorX/facturascripts/blob/6add3d0d9c6d6d4f7dbeea1c838cb900dc9af97d/Core/Controller/ListAttachedFile.php#L52



Carlos Garcia 7 months ago Maintainer

You're right. I have corrected it in this commit https://github.com/NeoRazorX/facturascripts/commit/a5e64bb5f29367e072dfc984e775731c6b3dd8f4

Thank you so much for everything

Minh 5 months ago Researcher

@admin, could you please assign cve for this report?

Carlos Garcia 5 months ago Maintainer

That option is hidden to me

Chat with us

Jamie Slome 5 months ago Admin

Sorted 👍

> Sign in to join this conversation