Stored XSS via SVG File in microweber/microweber

0

Valid Reported on Jul 6th 2022

Description

By uploading SVG files, the users can perform Stored XSS attack.

Payload

Copy the following code and save as filename.svg. `<x:script xmlns:x="http://www.w3.org/1999/xhtml">alert(document.domain)</x:script>`

Proof of Concept

[1] Login as admin.
[2] upload the payload injected SVG file at
`https://demo.microweber.org/demo/admin/view:modules/load_module:files`
[3] Copy the uploaded svg file url and open in new tab.
[4] XSS!

Impact

If an attacker can execute the script in the victim's browser via SVG file, they might compromise that user by stealing its cookies.

CVE
CVE-2022-2495
(Published)

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

Severity
Medium (6.8)

Registry
Other

Affected Version
1.2.19

Visibility
Public

Status
Fixed

Found by

Thwin Htet
@thwinhtetwin
pro

Fixed by

Peter Ivanov
@peter-mw
maintainer

This report was seen 682 times.

We are processing your report and will contact the **microweber** team within 24 hours.
5 months ago

Thwin Htet modified the report 5 months ago

Thwin Htet modified the report 5 months ago

We have contacted a member of the **microweber** team and are waiting to hear back
5 months ago

Peter Ivanov has marked this vulnerability as a duplicate of **22561bfd-a28f-474e-9bfd-7263c1b71133** 5 months ago

Hi, this issue has been already fixed

The disclosure bounty has been dropped ×

The fix bounty has been dropped ×

The researcher's credibility has increased: +2

Thwin Htet 5 months ago Researcher

Hello again.
I think my report is not a duplicate because this vulnerability is still exist on version 1.2.19.
Although server return 500 error, it still uploads the malicious SVG file successfully,
I have PoC video. If you still need a PoC video, i will share with you.

Peter Ivanov 5 months ago Maintainer

Hi, i see

I have added a fix in this commit, so you can make this issue as valid

https://github.com/microweber/microweber/commit/d35e691e72d358430abc8e99f5ba9eb374423b9f

@admin, can you make the issue as valid ?

Thwin Htet 5 months ago Researcher

So.. am i valid to have a CVE ID?

Peter Ivanov 5 months ago Maintainer

yes you can have CVE

Jamie Slome 4 months ago Admin

Thanks for getting in touch. We will have this issue sorted ASAP :)

Thwin Htet 4 months ago Researcher

@admin , can you please ask the maintainer to confirm that a fix has been merged and ready to proceed with the CVE?

Jamie Slome 4 months ago Admin

I have reverted the status of the report to `pending`.

@maintainer - please feel free to proceed with marking this report as `Valid and Fixed`. A CVE will automatically be assigned and published once this is done 👍

Peter Ivanov modified the Severity from High (8.4) to Medium (6.8) 4 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

Peter Ivanov validated this vulnerability 4 months ago

Thwin Htet has been awarded the disclosure bounty ✅

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Peter Ivanov marked this as fixed in 1.2.21 with commit d35e69 4 months ago

Peter Ivanov has been awarded the fix bounty ✅

This vulnerability will not receive a CVE ❌

Sign in to join this conversation