huntr

Unrestricted Upload of File with Dangerous Type in microweber/microweber

0

✓ Valid Reported on Mar 9th 2022

Description

Malicious user can bypass checking and upload .phtm or .php6 file which leads to stored XSS.

Proof of Concept

Step 1: Login as admin at https://demo.microweber.org/demo/admin/
Step 2: Go to Websites setting and Edit any page (https://demo.microweber.org/demo/admin/page/24/edit)
Under Pictures tag, choose Add files with content and extension below

.phtm

```
<a id=x tabindex=1 onfocus=alert(1) autofocus></a>
```

https://demo.microweber.org/demo/userfiles/media/default/123_7.phtm
https://drive.google.com/file/d/1eDNDRLquNuev0diRuMt3Z2cxKhEj5bt4/

.php6

```
<img src=x onerror=alert(origin)>
```

https://demo.microweber.org/demo/userfiles/media/default/123.php6
https://drive.google.com/file/d/15KatRGUfbCndq3oMHhUzjXosIfTGW908/

Impact

Stored XSS

CVE

CVE-2022-0912
(Published)

Vulnerability Type

CWE-434: Unrestricted Upload of File with Dangerous Type

Severity

Medium (4.8)

Visibility

Public

Status

Fixed

Found by

NCSC VN National Cyber Security Center

nhiephon

@nhiephon

master

Fixed by

Peter Ivanov

@peter-mw

maintainer

This report was seen 563 times.

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

Bozhidar Slaveykov validated this vulnerability 9 months ago

nhiephon has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Peter Ivanov marked this as fixed in **1.2.11** with commit **242452** 9 months ago

Peter Ivanov has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Chat with us

This vulnerability will not receive a CVE ✗

nhiephon 9 months ago Researcher

Hi Maintainer,

I think you have a bit of confusion in the patch. The extension to prevent is .phtm, .phtml has been blacklisted before.

Regards.

Sign in to join this conversation