enferas / XSS_pfesense.md

Created 2 months ago

☆ Star

<> Code -o-Revisions 1

XSS in pfsense v2.5.2

XSS_pfesense.md

XSS vulnerability in pfsense v2.5.2

The path of the XSS vulnerability in file https://github.com/pfsense/pfsense/blob/master/src/usr/local/www/vendor/filebrowser/browser.php

In this file we get the list of dirs and files in specific directory through the function get_content.

Then we print the list of files as we can see in this simplified code.

```
// ----- read contents -----
if (is_dir($path)) {
    list($dirs, $files) = get_content($path);
?>

//...

// ----- files -----
foreach ($files as $file):
    //...

    $fqpn = "{$path}/{$file}";

    if (is_file($fqpn)) {
        $fqpn = realpath($fqpn);
        $size = sprintf("%.2f KiB", filesize($fqpn) / 1024);
    } else {
        $size = "";
    }

?>
    <tr>
        <td></td>
        <td class="fbFile vexpl text-left" id="<?=$fqpn;?>">
            <?php $filename = htmlspecialchars(addslashes(str_replace("//","/", "{$p
            <div onClick="$('#fbTarget').val('<?=$filename?>'); loadFile(); $('#fbBr
                <img src="/vendor/filebrowser/images/file_<?=$type;?>.gif" alt="" ti
                &nbsp;<?=htmlspecialchars($file);?>
            </div>
        </td>
        <td class="vexpl text-right">
            <?=$size;?>
        </td>
    </tr>
```

There is no sanitizer with the variable $fqpn which contains the file name.

```
<td class="fbFile vexpl text-left" id="<?=$fqpn;?>">
```

The developer confirm the vulnerability with the current file name

''' touch '">{<}img src=src onerror=alert(3) foo=foo{>}' '''

The patch:
https://github.com/pfsense/pfsense/commit/73ca6743954ac9f35ca293e3f2af63eac20cf32e

enferas commented on Oct 3 Author

CVE-2022-42247 is assigned to this discovery