Bug 12226 - CSRF protection bypass with XSS

Status: CLOSED FIXED

Alias: None

Product: IPFire
Component: --- (show other bugs)
Version: 2
Hardware: all Linux

Importance: - Unknown - Security
Assignee: Michael Tremer
QA Contact:

URL: https://192.168.56.5:444/cgi-bin/mail...
Keywords:

Depends on:
Blocks:

Reported: 2019-10-30 09:28 UTC by Pisher Honda
Modified: 2020-01-22 21:08 UTC (History)
CC List: 3 users (show)

See Also:

Attachments	
using xss to craft a csrf request (107.96 KB, image/png) 2019-10-30 09:28 UTC, Pisher Honda	Details
poc for csrf (96.43 KB, image/png) 2019-10-30 09:31 UTC, Pisher Honda	Details
Add an attachment (proposed patch, testcase, etc.)	View All

Note
You need to log in before you can comment on or make changes to this bug.

Pisher Honda 2019-10-30 09:28:29 UTC **Description**

Created attachment 718 [details]
using xss to craft a csrf request

As the CSRF mitigation technique ipfire employed reffer header check technique but as the application is already vulnerable to xss i was able to bypass the refer check, here is how i did it

- Navigate to mail service under the system menu and enable it

- fill in the input fields in the field mail server address which is vulnerable to XSS(CSRF-1) , Now using this XSS vulnerability craft a post request to a page which is vulnerable to csrf(wake on lan)

Vulnerable Files ::
==================

cgi-bin/mail.cgi   is vulnerable for reflected XSS

Pisher Honda 2019-10-30 09:31:40 UTC **Comment 1**

Created attachment 719 [details]
poc for csrf

Michael Tremer 2019-10-30 11:00:33 UTC **Comment 2**

Thank you for reporting this.

Could you please verify for me that this patch fixes the problem?

> https://patchwork.ipfire.org/patch/2561/

Pisher Honda 2019-10-30 14:18:05 UTC **Comment 3**

Hey there,

This would patch the issue. I would like to know, if we can go ahead and request CVE for this issue? or else is there a procedure from your end to apply for a CVE?

Michael Tremer 2019-10-30 14:28:15 UTC **Comment 4**

(In reply to Pisher Honda from comment #3)
> This would patch the issue.

Did you just review the patch or did you test it, too?

> I would like to know, if we can go ahead and
> request CVE for this issue? or else is there a procedure from your end to
> apply for a CVE?

You can go ahead and request a CVE. We do not have a procedure for this as it is normally done by the researcher before the issue is being reported to us.

Pisher Honda 2019-10-30 15:49:17 UTC **Comment 5**

> Did you just review the patch or did you test it, too?

ijust reviewed the patch code. i didn't had much time to test it with DAST approach will test it tommorrow once i go to work space, Please send me the complete modified mail.cgi file(includes patch as well) so that i can quickly test it using DAST approach and get back to you

FYI
version used for testing is *IPFire 2.23 - Core Update 136*

Pisher Honda 2019-10-30 15:54:00 UTC **Comment 6**

(In reply to Michael Tremer from comment #4)
> (In reply to Pisher Honda from comment #3)

> it is normally done by the researcher before the issue is being reported to
> us.

This should not be the case, cve requests should be donee the vulnerability is patched

Peter Müller **2019-12-16 16:35:41 UTC** **Comment 7**

https://git.ipfire.org/?p=ipfire-2.x.git;a=commit;h=095bf494074994c5a2cd867f3b00603de95ed207

Peter Müller **2019-12-16 16:37:53 UTC** **Comment 8**

https://blog.ipfire.org/post/ipfire-2-23-core-update-138-released

Why didn't the release note of Core Update 138 mention this?

Michael Tremer **2019-12-16 17:31:50 UTC** **Comment 9**

(In reply to Peter Müller from comment #8)
> https://blog.ipfire.org/post/ipfire-2-23-core-update-138-released
>
> Why didn't the release note of Core Update 138 mention this?

Because it was not released in c138. It was supposed to be, but then everything was moved to 139 and an emergency update was inserted for the Intel vulnerabilities:

> https://git.ipfire.org/?p=ipfire-2.x.git;a=shortlog;h=refs/heads/core138

This is now scheduled to be released in c139.

Peter Müller **2019-12-17 20:58:08 UTC** **Comment 10**

Hi,

if this vulnerability is about to be fixed in C139, this bug should be classified as ON_QA, shouldn't it?

Thanks, and best regards,
Peter Müller

Peter Müller **2020-01-22 21:08:27 UTC** **Comment 11**

https://blog.ipfire.org/post/ipfire-2-23-core-update-139-released

Format For Printing - XML - Clone This Bug - Top of page