New issue

Jump to bottom

server side request forgery vulnerability in url uploader bypass CVE-2018-14728 by adding /favicon.ico to end of php file. #598

Open **hackoclipse** opened this issue on Mar 5, 2020 · 6 comments

hackoclipse commented on Mar 5, 2020 • edited

Good afternoon ResponsiveFilemanager,

When i was doing a security test for a client of mine i noticed in your newest version of
ResponsiveFilemanager 9.13.4 (in 9.14.0 the url upload is completly broken but it also exist there) internal server side request forgery by adding to any php "/image.ico".

to reproduce this i reccomand to install ResponsiveFilemanager 9.13.4 and not ResponsiveFilemanager 9.14.0 because the url file uploader is completly broken and doesn't work at all even with legit jpeg's, but this version is also vulnerble.

you need to have url_upload enabled and run the code on a apache server with default configurations.
now send as url

> http://0.xip.io/server-status/favicon.ico

when you send that go back to the file manager and you will see a ico.
download that file and rename favicon.ico to favicon.html.
if you now open that you will see the apache status page.
as you can see this is a clear indication that CVE-2018-14728 is bypassable.

how does this work:
there are a few problems here.
first you only use a regex to verify if it is a allowed url.
and in php files (and sometimes html files) it is allowed to extend the url.
this means if i would go to index.php/favicon.ico than the apache server would return index.php and not favicon.ico, but it would extend the url.
secondly i use dns pinning to bypass your miner filter to check if you send localhost because if you do a nslookup on "0.xip.io" you will get:

bl4ckh4ck5@bl4ckh4ck5-laptop:~/$ nslookup 0.xip.io
Server: 10.5.0.1
Address: 10.5.0.1#53

Non-authoritative answer:
Name: 0.xip.io
Address: 0.0.0.0

and 0.0.0.0 is localhost, but this method could also be used to access other ip's in the network.

a while back i created a potential patch against SSRF what might help against this problem:
https://github.com/hackoclipse/ssrf-patch
but i reccomand to make the design client side that the webbrowser downloads the image and than you use a xmlhttprequest to request the normal file upload, because that function isn't vulnerble.
i reccomand to fix both problems that url upload works again in 9.14.0 and that you fix this internal server side request forgery.
A CVE is already been requested.

Dear ragards,

bl4ckh4ck5
https://hackoclipse.com

hackoclipse commented on Mar 5, 2020 • edited Author

in version 9.14.0 it also bypasses the preg_match but a little lower it brakes because of a programming mistake:
https://github.com/trippo/ResponsiveFilemanager/blob/master/filemanager/upload.php#L73
so when that bug gets fixxed it's very likely it becomes vulnerble again.

hackoclipse changed the title ~~server side request forgery vulnerability in url uploader bypass CVE-2018-14728 by adding /favicon.ico to end of php file.~~ server side request forgery vulnerability in url uploader bypass CVE-2018-14728 by adding /favicon.ico to end of php file. on Mar 5, 2020

hackoclipse commented on Mar 5, 2020 • edited Author

later noticed 127.0.0.1 and 0.0.0.0 also worked but at the company i found this vulnerability i used 0.xip.io to bypass there firewall.

hackoclipse commented on Mar 5, 2020 • edited Author

hmm after looking closer i was able to find the commit what made the bug:
8478bd4
after this commit was done a bug was created that url upload doesn't work anymore in 9.14.0. (even latest commit)

hackoclipse commented on Mar 7, 2020 Author

cve assinged: CVE-2020-10212

hackoclipse commented on Mar 7, 2020 • edited Author

after more testing i noticed this method also work with extension blacklist enabled in the config.
it isn't specificly ico files that work any file what isn't blacklist'ed would work.

galaktipus commented on Sep 7, 2020

any commit fixing the issue above?

hackoclipse mentioned this issue on Apr 4, 2021

remote code execution vulnerability in ajax_calls.php in save_img action because of no validation on extension name. #600

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants