# Unrestricted Upload of File with Dangerous Type in firefly-iii/firefly-iii

0

Valid Reported on Oct 1st 2021

Description
file upload vulnerability in application

Proof of Concept
step to reproduce
1)login to application
2) goto https://demo.firefly-iii.org/create-from-bill/1
3) upload file any kind of file application accept
Reference PoC
1) https://i.ibb.co/9wWRnsf/Screenshot-12.png
2)https://i.ibb.co/68NRd4m/Screenshot-13.png

while creating new bill user is able to upload any kind of malicious file appliation.

code

```
<input multiple="multiple" helptext="Maximum file size: 64 MB" class="form-
```

Solution : define file type validation in client side of the application tc

## References

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

CVE
CVE-2021-3846
(Published)

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

Severity
Medium (6.3)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

@0xAmal
@0xamal
unranked

Fixed by

James Cole
@jc5
maintainer

This report was seen 472 times.

We have contacted a member of the firefly-iii team and are waiting to hear back a year ago

James Cole validated this vulnerability a year ago

@0xAmal has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

James Cole a year ago Maintainer

Unclear but validated nonetheless. A mime-type validation is in place and the demo user is not allowed to upload anyway.

The feedback to the user about a blocked upload is missing but I dont consider it a security issue

Is the list of mime types too wide perhaps? see https://github.com/firefly-iii/firefly-iii/blob/main/config/firefly.php#L225

Let me know

@0xAmal a year ago Researcher

i have checked was able to upload any kind of files please validate file extension in application side before submitting the request and also mime type as a second layer of protection for file upload kind of vulnerability.

James Cole a year ago Maintainer

The file extension is user input, I'm not going to rely on that. Mime type protection is already in place and works for me: local.ERROR: File "winrar-x64-602.exe" is of type "application/x-dosexec" which is not accepted as a new upload.

@0xAmal a year ago Researcher

To properly validate the file MIME you need to use finfo which internally uses finfo_open

Basically you use it the following way

```
/** Using finfo to just get the MIME type */
$finfo     = new finfo(FILEINFO_MIME_TYPE);

/** You will get extension along with the mime types */
$extension  = $finfo->file($file_tmp);
```

James Cole a year ago Maintainer

Ahhhh miscommunication there, thanks. Bad code on my part. API upload uses finfo, the bill form does not. Will be fixed!

@0xAmal a year ago Researcher

thanks sir

James Cole a year ago Maintainer

Already fixed: the UploadedFile class validates the mime type also using finfo. Did you spot any gaps?

@0xAmal a year ago Researcher

let me check wait

@0xAmal a year ago Researcher

issue resloved

James Cole marked this as fixed with commit a85b64 a year ago

James Cole has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Jamie Slome a year ago Admin

CVE published! 🎊

Sign in to join this conversation