11 receipt — 2 analyze — 3 evaluation — 4 alarm — 5 prize

title
KakaoTalk account takeover via malicious

Service name
카카오톡

Vulnerability Type
다수의 개인정보 노출

test environment
Android 10

Vulnerability Description
Hi,

In KakaoTalk 10.4.3 there are a couple of low-hanging fruit vulnerabilities which when combined together allow an attacker to steal another user's chat messages.

Please see the PDF report attached for the full details.

If you require additional info I can provide more details and test scripts, just let me know.

Cheers,

stulle123

Countermeasures
This is a list of countermeasures I get think of from the top of my head:
1) CommerceBuyActivity:
* Don't export it if not necessary
* Improve URL input validation so that an attacker cannot load arbitrary https://buy.kakao.com/ URLs
* Sanitize intent:// URIs (set Component and Selector to null) or disable the intent:// scheme all-together if not required

kakaotalk_report.zip

Please write a comment

SAVE

First, Thank you very much again for your awesome report and your ongoing engagement.

While we prefer not to disclose vulnerabilities publicly, we value and respect your perspective.

If you decide to write a blog post about this, we would appreciate it if you could consider masking any information that might reveal our company's identity, as a favor to us.

Best regards,

2024-03-15 03:06

Hi,

That's great news!

Since the issue is fixed now, I'd like to inform you that I will write a blog post about it.

Regarding publishing the blog post, this exclusive remedy of Article 18 allows me to do it as I haven't received a reward:

⑤ “회원"은 비밀유지 의무에 대한 동의를 거부할 수 있습니다. 다만, 이 경우 “프로그램" 이용이 불가능합니다.

Also, as stated in the Terms of Service, the program is applicable to Koreans only and in fact I don't have the Korean citizenship.

Before I publish the blog post online, I will share it with you.

2024-03-14 11:14

Hi,

The issue with the Android KakaoTalk has been resolved and the fix is included in version 1.9.0. Thank you for your continued interest in and support for our service.

2024-03-14 02:08

Hello again,

Did you fix the remaining bugs in the Android app?

Cheers,

stullenfoo

2024-03-12 12:14

inclusion in the previous release, due to unforeseen complications, it has been deferred to the upcoming release. Should you have any inquiries, please do not hesitate to reach out.

2024-02-19 02:22

Hi there,

Any updates?

I discovered that https://buy.kako.com is offline and that https://m.shoppinghow.kakao.com/m/product/W25927333803/view_type:image&q:%22%3E%3Cimg%20src=x%20onerror=alert(1);%3E is encoding double quotes now. So, the XSS vulnerability is fixed I believe.

Was the Android app fixed as well?

Cheers,

2024-02-18 12:47

Hi.
First of all, thank you for your continued interest.

We are currently addressing these vulnerabilities and expect to have them resolved within February. Please let us know if you require any further information or assistance.

Cheers,

2024-01-29 03:28

Hi!

Any updates? Have the vulnerabilities been addressed?

Thanks,

stullenfoo

2024-01-28 16:57

Thank you very much for your valuable feedback. We take suggestions from our users seriously and are committed to continually improving our services. Rest assured, your feedback will be thoroughly reviewed by our team and considered in our future enhancements.

Wishing you a prosperous and joyful new year!

2024-01-09 02:06

Hi Kakao Security Team,

Thanks for coming back to me.

Just some feedback regarding your bug bounty program:

I think it's very dangerous for your company if you limit the bounty reward to Korean citizens only.

This prevents international security researchers to disclose security vulnerabilities to you directly, but use other forms of *irresponsible* disclosure instead (underground forums, black market, etc.).

2024-01-08 20:47

Hello,
This is Kakao Security Team.

This vulnerability action is still in progress.
Please note.

1) CommerceBuyActivity
To be patch before February 2024.

2) m.shoppinghow.kakao.com
Action has been completed.

3) Kakao Mail Account
Measures are being discussed.

Thanks,
Kakao Security Team.

2024-01-03 02:16

Happy New Year!

Any news regarding the issue?

Have you patched the vulnerability in the latest KakaoTalk version?

Cheers

2024-01-02 15:44

Hi!

Can you let me know until when you plan to fix the issues?

With the next KakaoTalk release?

Thanks

2023-12-13 13:22

Hello Again,

First of all, I would like to ask you not to publish the blog post.
Kakao's Bug Bounty Program is basically based on the non-disclosure of information, so we cannot allow the disclosure of any information about vulnerabilities, regardless of whether they have been addressed.

Second, we don't have plans to request the CVE ID.

We understand that you are disappointed, but this is our company policy, so there's nothing we can do about it. Personally, I also find it quite regrettable.

Thank you for your understanding.

2023-12-13 06:37

Hi,

Thank you very much!

Please let me know when the vulnerability will be fixed so that I can publish a blog post.

Are you planning to request a CVE ID?

Cheers,

stulle123

2023-12-12 13:52

Kakao BugB

First of all, I want to express my sincere gratitude for the exceptionally well-crafted security report you submitted.

Your report has been identified as a vulnerability, and we are currently taking steps to address it by forwarding the details to the relevant department for necessary actions. Unfortunately, as per our bug bounty policy, rewards are only issued to domestic participants (Korean citizens).

However, KakaoTalk could be eligible for the GPSRP's reward criteria. Please keep this in mind, and we hope for positive results. Thank you very much for your interest in Kakao services.

GPSRP: https://bughunters.google.com/about/rules/5604090422493184/google-play-security-

2023-12-12 07:14

제외 상태로 변경되었습니다

2023-12-12 07:13

Hi,

Thanks for your reply.

I'm not a Korean citizen and I'm aware that no bounty will be paid out.

Cheers,

stulle123

2023-12-11 12:31