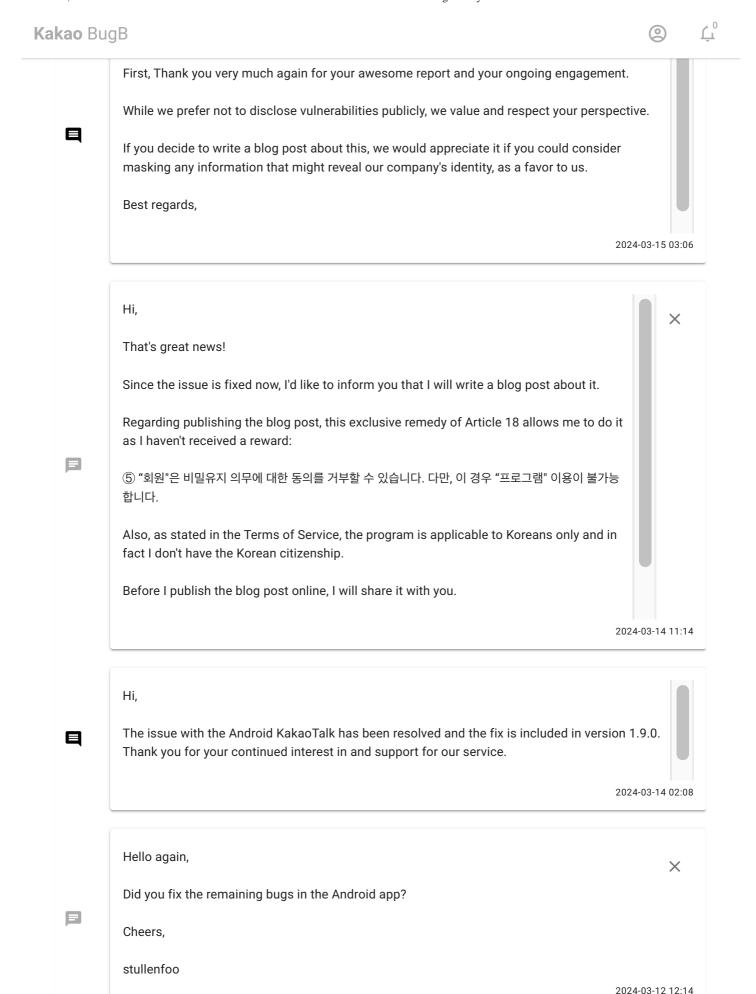
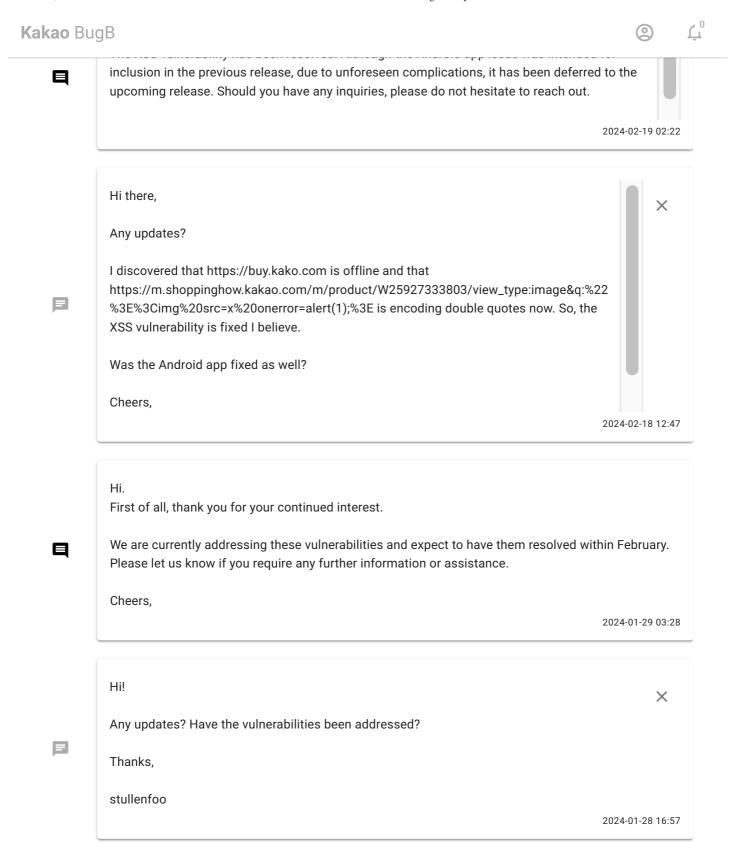
Kakao BugB TARGET **VULNERABILITY REPORTING** RANGE RULE FAQ 11 receipt 3 evaluation \_\_\_\_\_\_ 2 analyze 4 alarm 5 prize title KakaoTalk account takeover via malicious Vulnerability Type Service name 카카오톡 다수의 개인정보 노출 test environment Android 10 Mulnerability Description In KakaoTalk 10.4.3 there are 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 (0) Please write a comment SAVE •••

PRIVACY POLICY Copyright © Kakao Corp. All rights reserved.

TERMS OF USE

HALL OF FAME





## Kakao BugB







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

X

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.

m.shoppinghow.kakao.comAction has been completed.

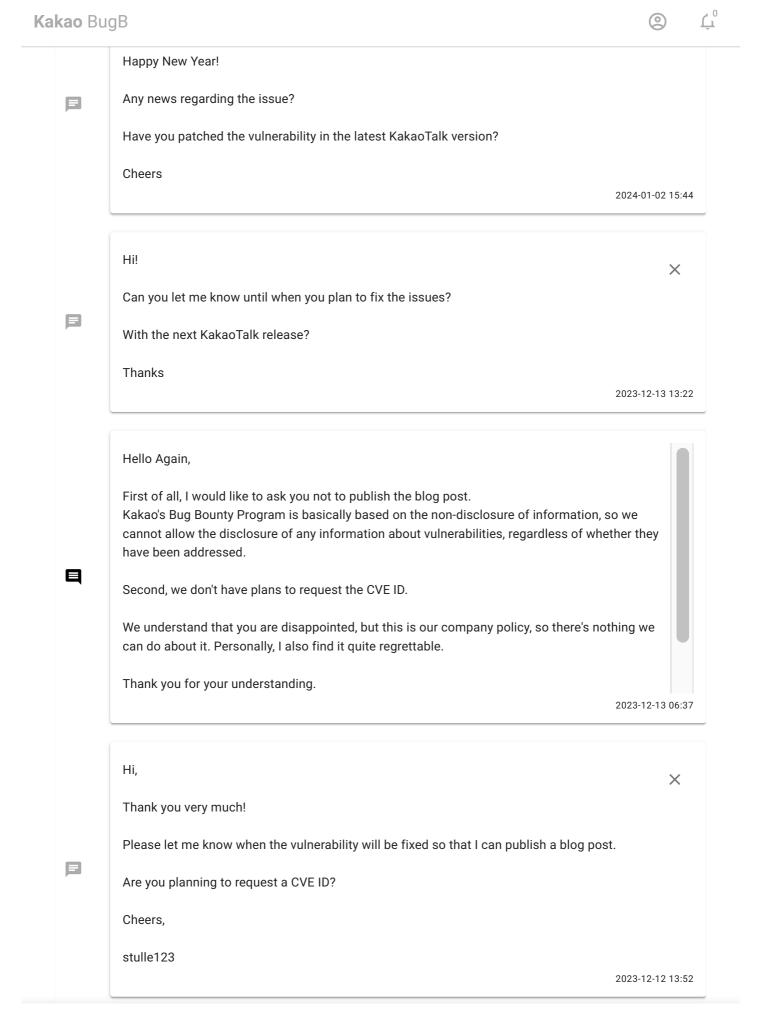
3) Kakao Mail Account

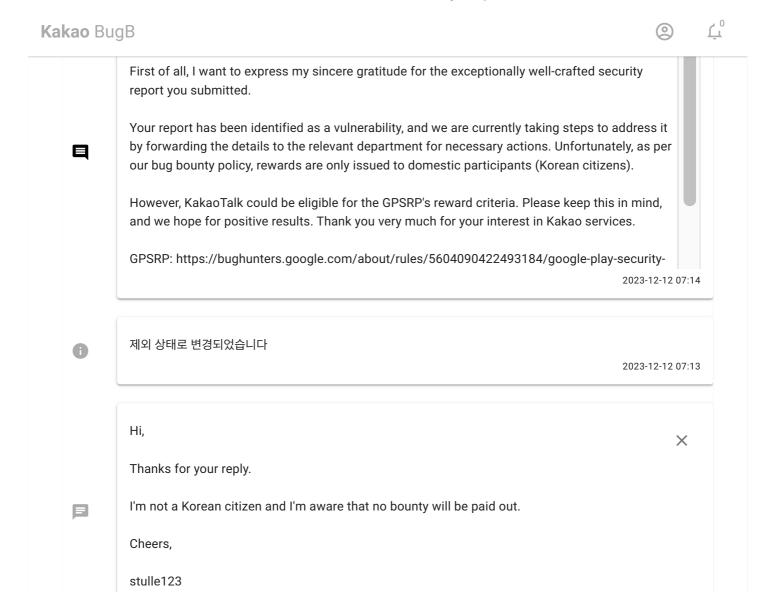
Measures are being discussed.

Thanks,

Kakao Security Team.

2024-01-03 02:16





2023-12-11 12:31