WHATSAPP - One Click Open Redirect via URL filtering bypass using at sign (@) [MEDIUM RISK]

Product: Whatsapp Messenger
Platforms: Web, iOS, Android
Vulnerability type: open redirect
Title: WHATSAPP - One Click Open Redirect via URL filtering bypass using at sign (@) [MEDIUM RISK]

Description

Complete details
By intercepting a request by Whatsapp's app to send a new message with a rich preview banner, and by replacing the banner's redirect url with a malicious URL, one can bypass the URL filtering of Whatsapp and send very misleading messages, such that can be very much used in sophisticated phishing attempts.
Through the usual flow, trying to send:

- https://facebook.com@instagram.com

Will result in the messenger attaching to the message a rich preview banner of instagram (as expected)
However, in this vulnerability, one replaces the original link in the message body with another - after the rich preview banner of the old link has already loaded.
So for example, if one writes in the message box:

- https://facebook.com

And lets the banner of facebook load, and then sends the message but not before intercepting the request and replacing:

- https://facebook.com

With:

- https://facebook.com@evil.com

The message that will appear at the victim's end will have the banner of facebook, but will successfully redirect to evil.com when is clicked, thus resulting in a dangerous open redirect that can be used in sophisticated phishing attacks.

This can easily be prevented by taking one of the 3 actions I have listed in the previous report A.K.A **"FACEBOOK - One Click Open Redirect via URL filtering bypass using at sign (@) [MEDIUM RISK]**" on Facebook.

Moreover, this allows accessing your forbidden https://evilzone.org as well (once is combined with this vulnerability and https://bit.ly service)

There is an actual risk in this vulnerability being open

Impact

MEDIUM RISK impact - using this, an attacker can send a malicious message to a victim, one that looks completely innocent and that seems to redirect to a legitimate website, which will redirect to any desired website instead.

Scenario:

- V(victim) gets a message from A(attacker) that looks innocent
- V believes this is a legitimate message based on its very legitimate appearance and clicks the message
- V is redirected to the malicious website instead of the actual twitter post, preferably a website that seems just like twitter in this case (classic phishing scenario)
    - The malicious website can be to a non secured website as well

Reproduction Steps

Users: A(attacker) , V(victim) [just 2 normal accounts]
Environment: private\group conversation between A and V where links sent by A are displayed as clickable to V (you should know the clickable link limitations of whatsapp)
Browser: Agnostic [ALL] (in Firefox, an interactive security warning is displayed to the user before allowing the redirection)
OS: Agnostic [ALL] (including native iOS/Android apps)
Description and Steps:

1. Open https://web.whatsapp.com/ on Chrome
2. Log in to A's account (you will need a phone for this)
3. Go on a conversation with V
4. Open devtools
5. Open the "search in all source files" tab
    i. Using Ctrl+Shift+F on Windows for example
6. Look for "t=e.id"
7. Enter file and pretiffy it
8. In the file, search "t = e.id"
9. Set a breakpoint at that line
10. Now use the web application to send a message to V
11. Paste the following: https://www.instagram.com/p/B6UH5FmlIOJ/
12. Wait for the preview banner to load
13. Press Enter and send the message
14. The breakpoint should hit. When that happens, paste the following to the console:
    i. [CODE]
        - *e.__x_body = e.__x_matchedText = 'https://instagram.com+cats_of_instagram&status=1200022932874&story=i_thought@bit.ly/35MBLeV?title=loving_cats&id=9832748932'*
    ii. [/CODE]
15. Now let the code continue by pressing F8 and let the abused message send
16. Open https://web.whatsapp.com/ on any browser / on the native iOS/Android apps
17. Log in to V's account (you will need another phone for this)
18. Go on a conversation with A
19. Click the message - either the banner, the image or the link is fine
20. See how you are redirected to *bit.ly/35MBLeV* instead of *https://twitter.com*
21. ATTACK IS SUCCESSFUL