RTLO Injection URI Spoofing

⚖ MIT license

☆ 85 stars    ⑂ 9 forks

☆ Star    ▾    🔔 Notifications

<> Code    ⊙ Issues    ⑂ Pull requests    ▷ Actions    ⊞ Projects    🛡 Security    📈 Insights

⑂ master ▾    Go to file

zadewg Update README.md   …    on May 7    🕐 21

View code

**README.md**

# RIUS - RTLO Injection URI Spoofing CVE-2020-20093; 20094; 20095; 20096, 2022-28345

**CWE-451: User Interface Misrepresentation of Critical Information.**
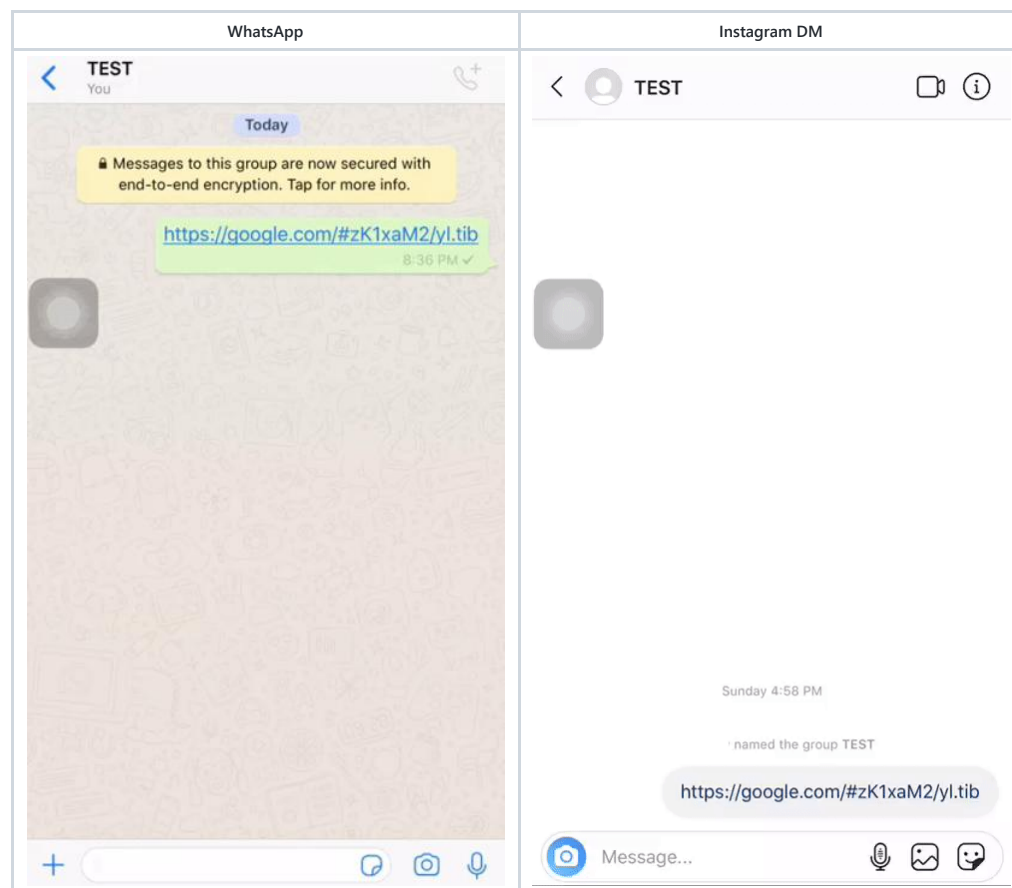
**CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')**

When a message contains a valid URL, it is highlighted and marked as hyperlink. However, this is printed to screen before sanitizing Unicode Control Characters, which results in URI spoofing via specially crafted messages.

Affects all recent distributions of iOS iMessage, WhatsApp, Instagram, and Facebook Messenger as of 2019.8.15

Patched in Signal iOS 5.34 release: commit

Patched in Telegram in 2019

| WhatsApp | Instagram DM |
|---|---|
|  |  |

**mapez** - telegram

## Releases

No releases published

## Packages

No packages published

## Contributors 2

- zadewg
- sickcodes sickcodes

## Languages

- Shell 66.4%
- Python 33.6%