

Framer Preview 12 Content Injection

Authored by [Julien Ahrens](#) | Site [rcesecurity.com](#)

Posted Sep 22, 2020

Framer Preview version 12 for Android exposes an activity to other apps called "com.framer.viewer.FramerViewActivity". The purpose of this activity is to show contents of a given URL via an fullscreen overlay to the app user. However, the app does neither enforce any authorization schema on the activity nor does it validate the given URL.

tags | advisory
advisories | [CVE-2020-25203](#)

SHA-256 | e54f0aa32e54c06b14955e19264b2f743bd0ebfed0a629f5cc6a8d1038c27426 [Download](#) | [Favorite](#) | [View](#)

[Related Files](#)

Share This

Like Tweet LinkedIn Reddit Digg StumbleUpon

[Change Mirror](#)

[Download](#)

RCE Security Advisory
<https://www.rcesecurity.com>

1. ADVISORY INFORMATION

Product: Framer Preview
Vendor URL: <https://play.google.com/store/apps/details?id=com.framerjs.android>
Type: Improper Export of Android Application Components [CWE-926]
Date found: 2020-09-06
Date published: 2020-09-22
CVSSv3 Score: 5.5 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:R/A:N)
CVE: CVE-2020-25203

2. CREDITS

This vulnerability was discovered and researched by Julien Ahrens from RCE Security.

3. VERSIONS AFFECTED

Framer Preview 12

4. INTRODUCTION

Framer Preview is the best way to view and interact with your Framer X and Framer Classic projects on Android phones and tablets.

(from the vendor's homepage)

5. VULNERABILITY DETAILS

The "Framer Preview" app for Android exposes an activity to other apps called "com.framer.viewer.FramerViewActivity". The purpose of this activity is to show contents of a given URL via an fullscreen overlay to the app user.

However, the app does neither enforce any authorization schema on the activity nor does it validate the given URL.

This can be abused by an attacker (malicious app) to load any website/web content into the fullscreen overlay. An exemplary exploit could look like the following:

```
Intent i = new Intent();  
i.setComponent(new ComponentName("com.framerjs.android", "com.framer.viewer.FramerViewActivity"));  
i.setAction("android.intent.action.VIEW");  
i.setData(Uri.parse("https://www.rcesecurity.com"));  
startActivity(i);
```

6. RISK

A malicious app on the same device is able to exploit this vulnerability to lead the user to any webpage/content. The specific problem here is the assumed trust boundary between the user having the Framer Preview app installed and what the app is actually doing/displaying to the user. So if the user sees the app being loaded and automatically loading another page, it can be assumed that the loaded page is also trusted by the user.

7. SOLUTION

-

8. REPORT TIMELINE

2020-09-06: Discovery of the vulnerability
2020-09-06: CVE requested from MITRE
2020-09-07: Contacted vendor via their security8, no response
2020-09-08: MITRE assigns CVE-2020-25203
2020-09-09: Informed vendor about the CVE assignment, no response
2020-09-22: Public disclosure due to unresponsive vendor

9. REFERENCES

-

File Archive: December 2022 <

| Su | Mo | Tu | We | Th | Fr |
|----|----|----|----|----|----|
| Sa | | | | | |
| | | | | 1 | 2 |
| 3 | | | | | |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | | | | | |
| 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | | | | | |
| 18 | 19 | 20 | 21 | 22 | 23 |
| 24 | | | | | |
| 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | | | | | |

Top Authors In Last 30 Days

Red Hat 150 files

Ubuntu 68 files

LiquidWorm 23 files

Debian 16 files

malvuln 11 files

nu11security 11 files

Gentoo 9 files

Google Security Research 6 files

Julien Ahrens 4 files

T. Weber 4 files

File Tags

ActiveX (932) December 2022
Advisory (79,754) November 2022
Arbitrary (15,694) October 2022
BBS (2,859) September 2022
Bypass (1,619) August 2022
CGI (1,018) July 2022
Code Execution (8,926) June 2022
Conference (673) May 2022
Cracker (840) April 2022
CSRF (3,290) March 2022
DoS (22,602) February 2022
Encryption (2,349) January 2022
Exploit (50,359) Older
File Inclusion (4,165)

File Upload (946)

Firewall (821) AIX (426)
Info Disclosure (2,660) Apple (1,926)
Intrusion Detection (867) BSD (370)

Java (2,899) CentOS (55)
JavaScript (821) Cisco (1,917)
Kernel (6,291) Debian (6,634)
Local (14,201) Fedora (1,690)
Magazine (586) FreeBSD (1,242)
Overflow (12,419) Gentoo (4,272)
Perl (1,418) HP-UX (878)
PHP (5,093) IOS (330)
Proof of Concept (2,291) iPhone (108)
Protocol (3,435) IRIX (220)
Python (1,467) Juniper (67)
Remote (30,044) Linux (44,315)
Root (3,504) Mac OS X (684)
Ruby (594) Mandriva (3,105)
Scanner (1,631) NetBSD (255)
Security Tool (7,777) OpenBSD (479)
Shell (3,103) RedHat (12,469)
Shellcode (1,204) Slackware (941)
Sniffer (886) Solaris (1,607)

Systems

[Login](#) or [Register](#) to add favorites

- Spoof (2,166)

SQL Injection (16,102)

TCP (2,379)

Trojan (686)

UDP (876)

Virus (662)

Vulnerability (31,136)

Web (9,365)

Whitepaper (3,729)

x86 (946)

XSS (17,494)

Other
- SUSE (1,444)

Ubuntu (8,199)

UNIX (9,159)

UnixWare (185)

Windows (6,511)

Other

Site Links


- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory

About Us


- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By

Rokasec



Follow us on Twitter



Subscribe to an RSS Feed