Android o2 Business 1.2.0 Open Redirect

Authored by Julien Ahrens | Site rcesecurity.com

Posted Jul 3, 2020

o2 Business for Android version 1.2.0 suffers from an open redirection vulnerability.

tags | exploit
advisories | CVE-2020-11882
SHA-256 | ed073540b55db066df4e43d61452b19af671d57a6dad0ef1271c98600b232356 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
RCE Security Advisory
https://www.rcesecurity.com


1. ADVISORY INFORMATION
========================
Product:        o2 Business for Android
Vendor URL:     https://play.google.com/store/apps/details?id=telefonica.de.o2business
Type:           Open Redirect [CWE-601]
Date found:     2020-04-16
Date published: 2020-07-01
CVSSv3 Score:   3.3 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N)
CVE:            CVE-2020-11882


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


3. VERSIONS AFFECTED
====================
o2 Business App for Android 1.2.0


4. INTRODUCTION
===============
Kommunikation ist Ihr tägliches Sprungbrett in die Geschäftswelt. Und mit der
neuen O2 Business App haben Sie alle wichtigen Details stets vor Augen.
Verfolgen Sie investierte Gesprächszeiten zurück und sehen Sie verfügbare
Kommunikations-Kapazitäten vorher. Vom aktuellen Stand des Inklusiv-Volumens,
über Einzelverbindungen und Tarifdetails, bis zur lokalen Netz-Qualität behalten
Sie mit der O2 Business App immer und überall den Durchblick. Erfahren Sie jetzt
mehr über Ihren informativen Begleiter!

(from the vendor's homepage)


5. VULNERABILITY DETAILS
========================
The "O2 Business App" for Android exposes an activity to other apps called
"canvasm.myo2.SplashActivity". The purpose of this activity is to handle
deeplinks which can be delivered to the app either via links or by directly
calling the activity.

However, the app does not properly validate the format of deeplinks by just
using str.contains() to verify the allowed host:

private boolean isVanityLink(String str) {
        return str.contains("https://o2.de") || str.contains("https://blau.de")
        || str.contains("https://e2e2.o2.de") ||
        str.contains("https://e2e2.blau.de");
    }

private boolean isDeepLink(String str) {
    return str.contains("https://www.o2online.de")
    || str.contains("https://www.blau.de")
    || str.contains("https://e2e2.o2online.de")
    || str.contains("https://e2e2.blau.de")
    || str.contains(BuildConfig.PIRANHA_BASE_E2E2_URL)
    || str.contains("https://login.o2online.de")
    || str.contains("https://login-e2e2.blau.de")
    || str.contains("https://login.blau.de");
}

This can be abused by an attacker (malicious app) to redirect a user to any page
and deliver any content to the user. An exemplary exploit could look like the
following:

Intent i = new Intent();
i.setComponent(new ComponentName("telefonica.de.o2business", "canvasm.myo2.SplashActivity"));
Uri uri = Uri.parse("https://www.rcesecurity.com?dummy=https://o2.de");
i.setData(uri);
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 o2 Business app installed and what the app
is actually doing/displaying to the user. So if the user sees the app being
loaded and automatically redirecting to another page, it can be assumed that the
loaded page is also trusted by the user.


7. SOLUTION
===========
Update the app to version 1.3.0


8. REPORT TIMELINE
==================
2020-04-16: Discovery of the vulnerability
2020-04-16: Although Telefonica runs a VDP on Bugcrowd
(https://bugcrowd.com/telefonicavdp), I did not want to accept their non-
disclosure terms, which is why I have tried to contact them directly via their
official CERT contact.
2020-04-16: Telefonica responds and asks for full vulnerability details
2020-04-16: Send over the full advisory including a full PoC exploit.
2020-04-16: Telefonica acknowledges the issue
2020-04-16: CVE requested from MITRE
2020-04-17: MITRE assigns CVE-2020-11882
2020-06-03: No further communication from Telefonica. Mailed them again about
the status of the fix.
2020-06-03: Telefonica is still working on this issue and the fix is scheduled
to be included in the next release.
2020-06-04: Version 1.3.0 is released
2020-07-01: Public disclosure.


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 154 files
Ubuntu 73 files
LiquidWorm 23 files
Debian 18 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

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

packet storm

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