

Concerned with tampered APK sources on Play Store

High maxieds published GHSA-8q77-7hq8-f7g6 on Aug 25, 2020

Package

com.maxieds.chameleonminilivedebugger

Affected versions

1.1.6

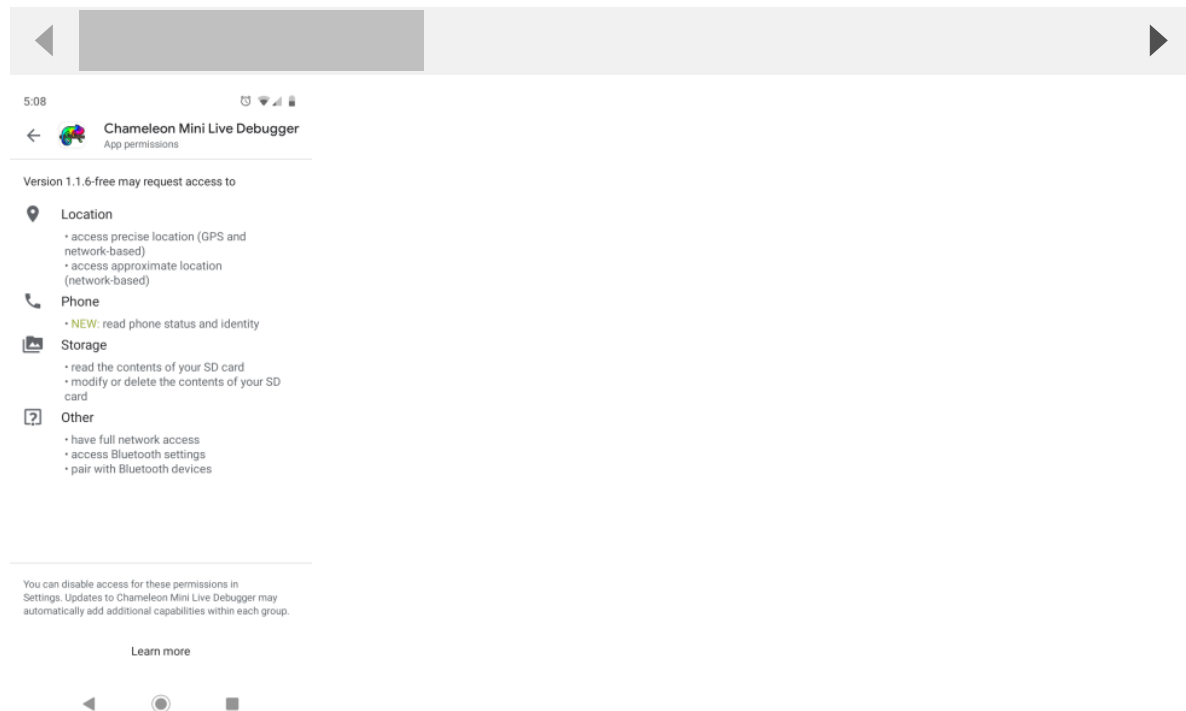
Patched versions

1.1.8

Description

In light of today's spirit debate with a few men of feeble mind (so to speak), but I33t hacking skills as it were (see [here](#) and [here](#)), I am concerned about the following new permission that showed up in v1.1.6-free of this app on Play Store today:

```
<?xml version="1.0" encoding="UTF-8"?><manifest versionCode="78" versionName="1.1.6-free" installLocation="2" compileSdkVersion="29" compileSdkVersionCodename="10" package="com.m
<uses-sdk minSdkVersion="26" targetSdkVersion="29"/>
<protected-broadcast name="android.hardware.usb.action.USB_STATE"/>
<uses-permission name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission name="android.permission.WRITE_SETTINGS"/>
<uses-permission name="android.permission.INTERNET"/>
<uses-permission name="android.permission.USB_PERMISSION"/>
<uses-permission name="android.permission.BLUETOOTH"/>
<uses-permission name="android.permission.BLUETOOTH_ADMIN"/>
<uses-permission name="android.permission.ACCESS_COARSE_LOCATION"/>
<uses-permission name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-feature name="android.hardware.usb.host" required="true"/>
<uses-feature name="android.hardware.bluetooth" required="false"/>
<uses-permission name="android.permission.READ_PHONE_STATE"/>
<application theme="AppThemeGreen" label="Chameleon Live Logger" icon="res/mipmap-anydpi-v26/chameleon_app_icon_round.xml" manageSpaceActivity=".LiveLoggerActivity" excludeFrom
<uses-library name="com.android.future.usb.accessory"/>
```

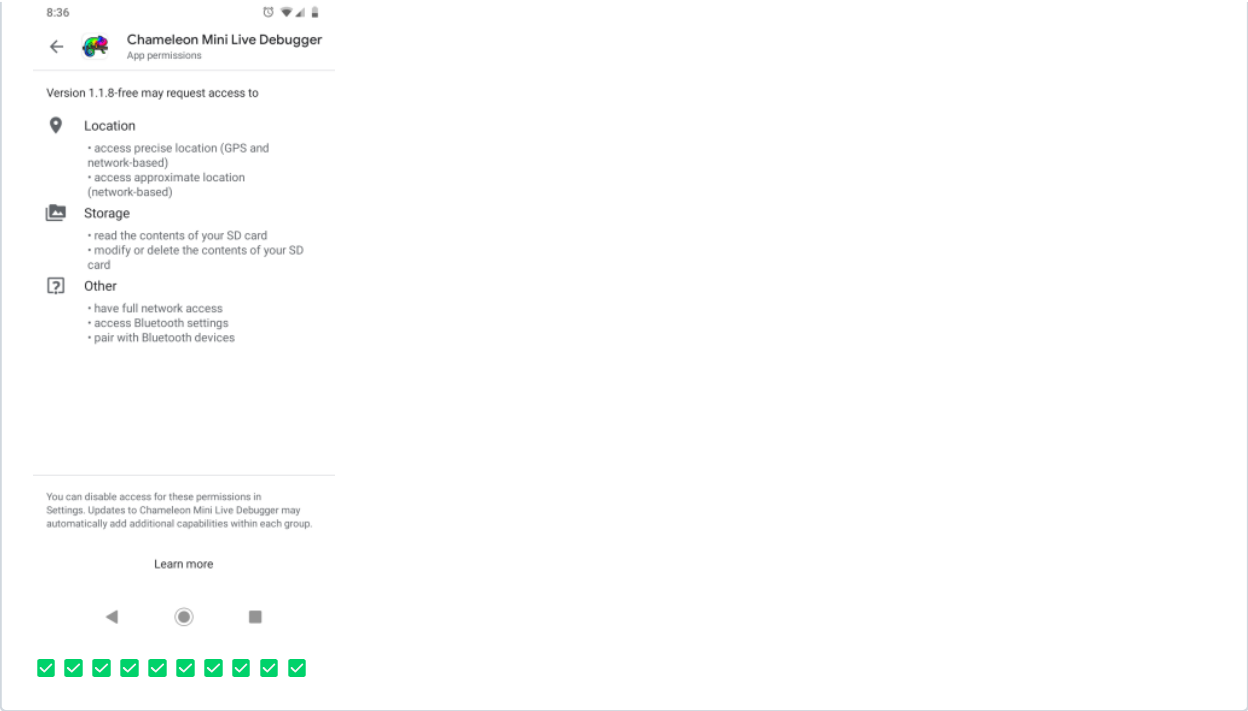


I have done my best by [reporting my own app to Google](#), submitting a developer issue to their support team on their console, and submitted a new v1.1.8-free app for rollout. **Please upgrade to v1.1.8 ASAP!**

[com.maxieds.chameleonminilivedebugger_1.1.6-free_0_AndroidManifest.xml.txt](#)
[com.maxieds.chameleonminilivedebugger_1.1.6-free.apk.zip](#)

=====

Back to normal with the just now launched v1.1.8 APKs on Play Store. **Again, PLEASE UPDATE TO THE NEW VERSION IMMEDIATELY!** This should quickly go into effect for both the `free` and `paid` flavors of the application. Users who have chosen to roll their own from source should be safe. Same for users that typically install directly from the signed APK sources on the [releases page](#).



Severity

High

CVE ID

CVE-2020-15165

Weaknesses

No CWEs