Android 4.4.2 Secure USB Debugging Bypass

03/07/2014

Software:	Android
Affected Versions:	Android 4.2.2-4.4.2
CVE Reference:	
Author:	Henry Hoggard - MWR Labs (https://labs.mwrinfosecurity.com/)
Severity:	Medium
Vendor:	Android
Vendor Response:	Fixed in Android 4.4.3

Description:

Android Developer Bridge (adb) is a command line tool that allows users to communicate with and debug the device. It gives users permissions to access many areas of the device, including the ability to manage apps, access device logs, read device input, take backups and execute OS commands. In Android 4.2.2, Google implemented Secure USB Debugging, aimed to prevent adb from being connected to malicious computers. The user has to authorize a computer before it can connect with adb. The idea is that users can only authorize a computer after entering the password and unlocking the device. The bug detailed is only exploitable when adb is enabled on the device.

Impact:

If adb is enabled on the device, attackers with physical access to a device can bypass Android's secure USB debugging protection. This allows attackers to gain adb access to the device, which would allow them to:

- Install/uninstall applications
- Bypass the lock screen
- Access a high privilege shell on the device
- Steal data from applications and settings on the device

Cause:

The adb authorize host popup is displayed prior to unlocking the device on the emergency dialer and lock screen camera. This allows attackers with physical access to authorize their computer and connect with adb.

Interim Workaround:

If you are running a vulnerable version of Android, it is recommended to disable ADB to prevent this attack.

Solution:

Android 4.4.3 prevents the adb authorization confirmation dialog from being opened in the emergency dialer and lock screen camera prior to unlocking the device. Users can now only authorize a computer with ADB after the lock screen stage is passed. Therefore it is recommended that a strong device password is used.

Technical details

The intended design of secure USB debugging, is that the user needs to be unlock the device to be able to authorize new adb hosts. If the user attempts to use adb while still at the Android lock screen, it will throw the following error:

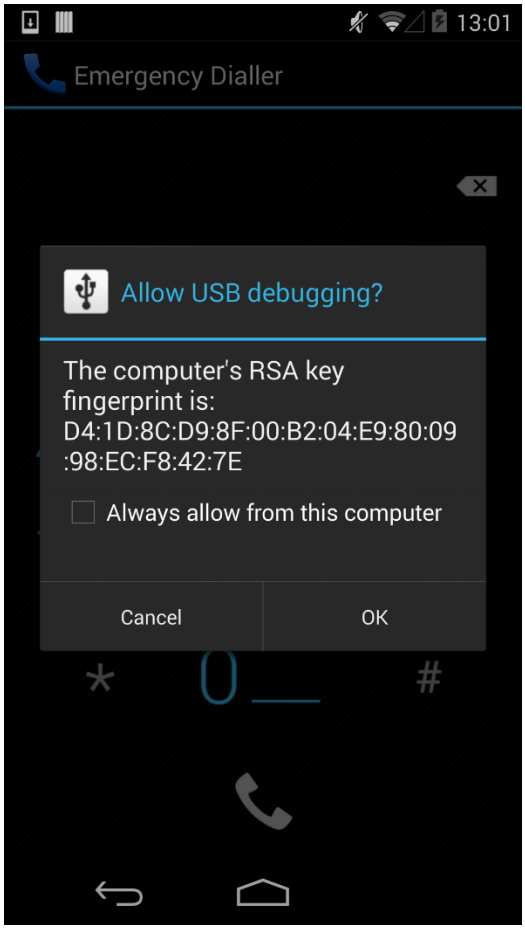
```
error: device unauthorized. Please check the confirmation dialog on your device
```

MWR discovered that by navigating to either the emergency dialer or the lock screen camera, then typing the below commands, it was possible to trigger confirmation dialog, the attacker could then accept this dialog and gain adb access to the device without knowing the device password.

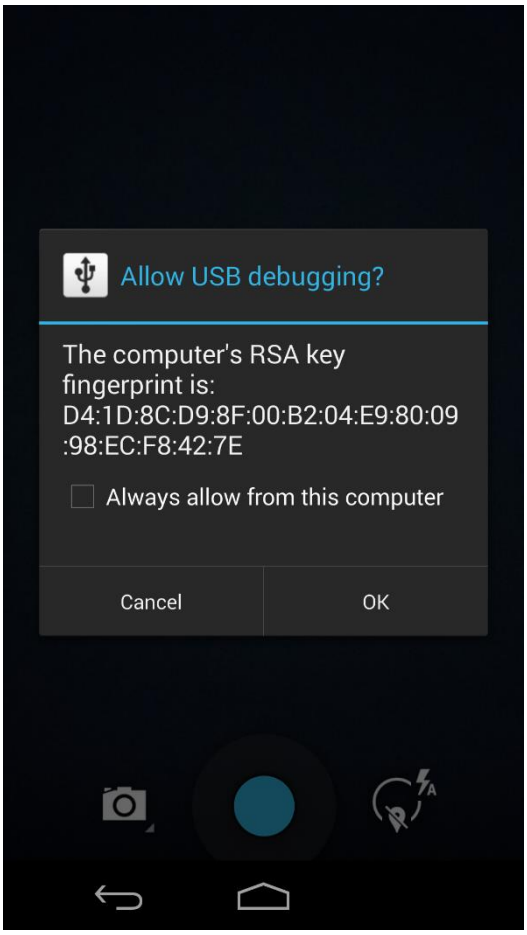
```
$ adb kill-server
$ adb shell
```

After gaining adb access to the device, to bypass the lock screen the following command is used:

```
$ adb shell pm clear com.android.keyguard
```



USB Debugging popup on emergency dialer



USB Debugging popup on lock screen camera

Detailed Timeline

Date:	Summary:
26/02/14	Reported to Google
27/02/14	Google start investigating issue.
29/04/14	Google replied stating that a patch has been created.
04/06/14	Android 4.4.3 officially released containing patch.