CVE-2015-1805 Google Android

Jyotsna Sharma

jyotsna.sharma@berkeley.edu

INTRODUCTION AND ANALYSIS OF THE FLAW

On March 18, 2016 a security advisory was published by Google for a critical vulnerability CVE-2015-1805 that applied to rooting apps. This fault allows malicious apps to gain "root" access to all Android phones with a below kernel version 3.18. The devices that do not receive patches anymore, or the ones with longer rollout time are greatly affected by this vulnerability. Google became aware of a rooting application using an unpatched local elevation of privilege vulnerability in the kernel on some Android devices (CVE-2015-1805). For this application to affect a device, the user must first install it.[3,2] This advisory applies to all unpatched Android devices on kernel versions 3.4, 3.10 and 3.14, including all Nexus devices. Android devices using Linux kernel version 3.18 or higher are not vulnerable. [2]

Figure 1: Google Android

The vulnerability is ranked as critical and can be exploited by rooting applications that users have installed on their devices to elevate privileges and run arbitrary code on the vulnerable device. The security flaw is very old, it was discovered in the upstream Linux kernel years ago and was fixed in April 2014. Unfortunately, the flaw was underestimated until the time C0RE Team reported to Google that it was possible to exploit it to target the Android OS.[3] Google has collected evidence of this vulnerability being abused on a Nexus 5 using a publicly available rooting tool, but there is no malicious exploitation of the security flaw. [3]

EXPLOITS

This vulnerability was implemented as a successor rooting solution when PingPongRoot was no longer working.The vulnerability can be traced back to the Linux kernel file *fs/pipe.c* function *pipe_iov_copy_to_user*. If *pipe_iov_copy_to_user* fails, the function goes to a redo routine that uses the same source buffer and copies it after the last position where the failed copy. This makes the destination *iovec* array overrun with the size of data the first step copied.[1]

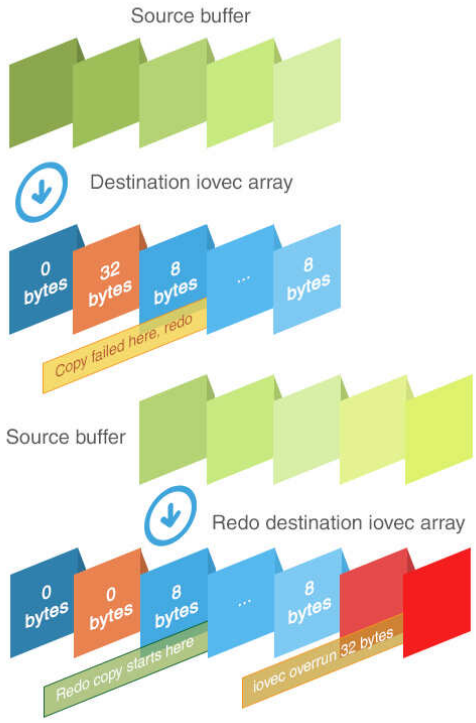

Figure 2: iovec overrun

The overrun situation causes an undefined memory access which leads to a denial of service. However, tricks are being used by this exploit which are capable of preventing system crash. For instance, if the total length of *iovec* array is set larger than the source buffer size which in default equals to *PIPE_BUF of 4096* bytes, overrun can be avoided in redo routine. This then continues the "for" loop to enter *pipe_iov_copy_to_user* for a third time to

copy the remaining data. This time, it triggers the overrun accessing data beyond the end of the *iovec* buffer which is sprayed with *iovec* and *iov_base* set to a kernel address. [1]

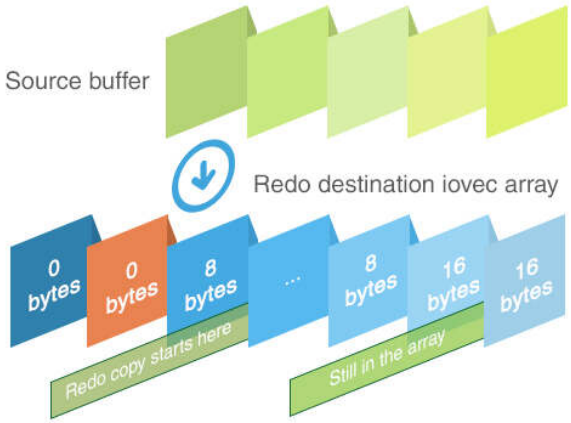

Figure 3: Preventing crash in the redo

Unlike a redo routine, this step uses *__copy_to_user_inatomoc* instead of protective *copy_to_user* to achieve kernel memory arbitrary write. This is the reason why it did not trigger the overrun in the redo. [1]

REMEDIATION

Installation of rooting applications that make use of this vulnerability has been blocked — both within Google Play Store and outside of Google Play — using Verify Apps. In addition to this, user systems were updated to detect applications that use this specific vulnerability.

To provide a final layer of defense for this issue, partners were provided with a patch for this issue on March 16, 2016. Nexus updates were being created and released a few days later. Source code patches for this issue have been released to the Android Open Source Project (AOSP) repository. [2]

The following are mitigations that reduced the likelihood users that were impacted by this issue:

- Verify Apps had been updated to block the installation of applications that Google learned were attempting to exploit this vulnerability both within and outside of Google Play. [2]
- Google Play does not allow rooting applications, like the one seeking to exploit this issue. [2]
- Android devices using Linux kernel version 3.18 or higher were not vulnerable. [2]

To mitigate the risk of exposure, users should have on their Android devices a security patch level of March 18, 2016, or a security patch level of April 2, 2016 and later. [3]

REFERENCES

[1] https://www.trendmicro.com/en_us/research/16/c/critical-cve-2015-1805-vulnerability-allows-permanent-rooting-android-phones.html
[2] https://source.android.com/security/advisory/2016-03-18
[3] https://securityaffairs.co/wordpress/45507/mobile-2/android-cve-2015-1805-fixed.html