Android vulnerabilities attacking Nexus 6 and 6P custom boot modes

By Roee Hay

Published: 2017-01-05 · Archived: 2026-04-05 19:22:13 UTC

Roee Hay

X-Force Application Security Research Team Leader

IBM Security

Co-authored by Michael Goberman.

In recent months, the X-Force Application Security Research Team has discovered several previously undisclosed Android vulnerabilities. The November 2016 and January 2017 Android Security Bulletins included patches to one high-severity vulnerability, CVE-2016-8467, in Nexus 6 and 6P. Our new paper, "Attacking Nexus 6 & 6P Custom Bootmodes," discusses this vulnerability as well as CVE-2016-6678.

Custom Boot Modes

The paper describes how an attacker can use PC malware or malicious chargers to reboot a Nexus 6 or 6P device and implement a special boot configuration, or boot mode, which instructs Android to turn on various extra USB interfaces.

Accessing the Nexus 6 Modem Diagnostics

These interfaces, notably the modem diagnostics interface, give attackers access to additional functionalities. This allows them to take over the Nexus 6 modem, thus compromising confidentiality and integrity.

Access to the modem enables attackers to intercept phone calls, for example. The image below depicts the waveform of the receive channel of a successfully intercepted phone call:

Attackers can also sniff mobile data packets. The image below illustrates how we successfully sniffed Long-Term Evolution (LTE) data:

Furthermore, this level of access to the Nexus 6 modem allows attackers to find the exact GPS coordinates with detailed satellite information, place phone calls, steal call information and access or change nonvolatile (NV)

items or the EFS partition.

Triggering the Android Vulnerabilities

The PC malware or malicious charger can boot the Nexus 6/6P device with the special boot mode configuration if Android Debug Bridge (ADB) is enabled on the device. Developers use ADB for debugging, and users leverage it to sideload Android application packages (APKs) onto their devices. Once connected, the victim must authorize the PC or charger on the device if it wasn't permanently authorized before the attack. Then, the attacker can simply issue the following commands:

```
adb reboot bootloader
fastboot oem config bootmode bp-tools (N6)
fastboot oem bp-tools-on (N6, option 2)
fastboot oem enable-bp-tools (N6P)
fastboot reboot
```

These commands will reboot the device with the special boot mode that enables the interfaces. Every future boot from this point forward will have the boot mode configuration enabled. This means the attack is persistent and no longer requires ADB to run, although it still requires USB access. Therefore, the attacker only needs the victim to enable ADB once. Moreover, a lucky attacker might wait for the device to be in fastboot mode, which requires no authorization from the victim. This, however, is less likely.

In addition to the above boot mode changing technique, there is another way for physical attackers to boot the device with a custom boot mode. An attacker with physical access to a device can reboot it into the fastboot mode and select BP-Tools or Factory to set the relevant boot mode configuration, as illustrated below:

Accessing the Modem AT Interface

The vulnerability affects the Nexus 6P less severely because the modem diagnostics are disabled in the modem's firmware, which prohibits the nefarious activities described above. There are, however, additional USB interfaces that attackers can access, such as the modem AT interface, which is also vulnerable in Nexus 6. By accessing that interface, an attacker can send or eavesdrop on SMS messages and potentially bypass two-factor authentication.

An attacker can also access phone call information, change various radio settings and much more.

ADB Access

The vulnerability in 6P enables the ADB interface even if it was disabled in the developer settings user interface (UI). With access to an ADB-authorized PC, a physical attacker could open an ADB session with the device and cause the ADB host running under the victim's PC to RSA-sign the ADB authentication token even if the PC is locked.

Such an ADB connection would enable an attacker to install malware on the device. PC malware on an ADB-authorized machine might also exploit CVE-2016-8467 to enable ADB and install Android malware. The PC malware waits for the victim to place the device in the fastboot mode to exploit the vulnerability.

Uninitialized Kernel Memory Leakage in Nexus 6

Upon further analysis, we found that another suspicious USB interface is enabled in Nexus 6 when booted with the custom boot mode. The interface identifies itself as “Motorola Test Command.” The kernel driver responsible for this interface is f_usbnet. Interestingly, this driver brings up an Ethernet-over-USB adapter, which can be configured from the host end. This allows for some exfiltration of network traffic.

We also discovered a vulnerability in the f_usbnet driver itself, identified as CVE-2016-6678, in which 4–5 bytes of uninitialized kernel data are padded to every Ethernet frame carried over USB. This leak may contain sensitive data that could empower cybercriminals to exploit the system. The image below illustrates an ICMP frame that contains the leak:

Coordinated Disclosure

The X-Force team responsibly disclosed these Android vulnerabilities to Google prior to the publication of this blog.

Google assigned a high level of severity to CVE-2016-8467 and mitigated it by forbidding a locked bootloader to boot with the dangerous boot modes. The first secure bootloader version of Nexus 6 is 71.22, released in the November 2016 Android Security Bulletin. The first secure bootloader version of Nexus 6P is 03.64, which was released as part of the January 2017 bulletin.

Google assigned moderate severity to CVE-2016-6678 and mitigated it by zeroing out the padding so that uninitialized bytes won’t leak. The patch was released as part of Android’s October 2016 bulletin.

Read the full paper: Attacking Nexus 6 & 6p Custom bootmodes
