**Google Patches Boot Mode Vulnerability in Android**

Recently, a critical vulnerability that attacked Nexus users in boot mode, subjected these devices to privilege escalation and denial of service attacks. The attackers could reboot the device into custom boot mode and then spy on their data or carry out remote attacks. With its android app security testing and vulnerability management, Google has now resolved the issue and fixed the vulnerability.

The vulnerability, known as CVE-2016-8467 allows hackers to use malicious chargers or PC malware to reboot Nexus 6 or Nexus 6P devices and then start in a customized boot configuration, which then commands Android to turn on extra USB interfaces.

Stating further details of the vulnerability in a blog post, IBM security researchers explained that it allows attackers to gain access to interfaces that give more control over an infected device. The main concern is of modem diagnostics interface in Nexus 6 as access to it enables hackers to access the modem, thus compromising the confidentiality and integrity of the device. Once the model is accessed, attackers can carry a number of tasks, such as intercepting a phone call, sniffing mobile data packets and grabbing information of GPS coordinates to track the device, make phone calls and steal call information, etc.

According to IBM, enabling Android Debug Bridge (ADB) allows a malicious charger or malware to boot the target in specific boot mode configuration. When connected, user will be forced to permanently accept the charger or PC, is issued some commands, and the device gets rebooted. After this, every time the device boots, it will automatically have the boot mode configuration enabled, thus no longer requiring ADB to run, and rather only requiring access to USB. Furthermore, with additional USB interfaces included in these devices, attackers can use them for sending and receiving SMS, bypass two-factor authentication and access a range of mobile device features and vulnerable apps that have not undergone android app security testing.

The vulnerability has now been patched by Google by disallowing locked bootloader to boot with risky boot modes.