## 华为、三星等手机 Bootloader存在多个漏洞

California大学的研究团队发现主流手机平台的bootloader中存在代码执行和DOS的安全漏洞。

研究者用BootStomp发现了6个新发现的漏洞，其中5个分别被厂商确认。还有一个之前报告过的安全缺陷。

在2017年USENIX大会上的一篇文章（[BootStomp: On the Security of Bootloaders in Mobile Devices](https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-redini.pdf)）中，专家表示这些安全问题会影响厂商提供的信任链（Chain of Trust）中的Trusted Boot 和 Verified Boot机制。

该过程应当可以有效地防止攻击者获取操作系统全部控制权，然而研究者发现当bootloader接受到来自攻击者的不可信的输入时，许多信任链的验证步骤就无效了。

这些漏洞中有的允许攻击者作为bootloader的一部分执行二进制代码，攻击者也可以进行永久的DOS攻击。研究人员开发的工具BootStomp能识别出两个bootloader的漏洞，攻击者可以在root权限下利用这两个漏洞解锁设备并打破信任链。

一般来说，bootloader不是开源的，因此进行分析比较困难，尤其是有目标平台外的动态分析。因此，研究者开发了自己的分析工具BootStomp，BootStomp结合了静态分析技术和限制下的象征性执行来建立多标签的标记分析来识别bootloader中的漏洞。

研究人员分析了bootloader在华为 P8 ALE-L23 (海思芯片)，索尼Xperia XA (联发科芯片)， Nexus 9 (NVIDIA芯片)，和两款基于LK的bootloader (高通芯片)平台的运行情况。

研究人员在华为P8的Android bootloader中发现了5个重要的漏洞，分别是任意内存写和分析保存在boot分区的Linux设备树（DTB）漏洞，读root可写oem\_info 分区时的堆溢出漏洞，root用户可写nve 和 oem\_info分区漏洞，可以导致永久性的rootkit安装的内存错误漏洞，允许攻击者像bootloader一样运行任意代码的任意内存写漏洞。

BootStomp还发现了NVIDIA hboot和高通aboot中的漏洞。NVIDIA hboot漏洞运行在EL1层，在硬件上相当于有Linux kernel的权限。高通aboot中的漏洞（CVE-2014-9798）之前已经被报告过可以被利用进行DOS攻击。

这些漏洞的利用依赖攻击者在non-volatile memory（非易失性存储器）上进行写操作的能力，bootloader也要从non-volatile memory中进行读操作，因此研究者提出利用新设备的硬件特征来禁止攻击者写操作等方法来解决这些漏洞的利用问题。