androidcentral.com

17/12/2012 21:51

The Samsung Exynos kernel exploit - what you need to know

SAMSUNG
8:53 PM
Voodoo Anti ExynosMemAbuse
EXYNOS MEM ABUSE VULNERABILITY STATUS
Okay :)
Your system is not currently vulnerable to this exploit
ENABLE VULNERABILITY FIX
ABOUT & CREDITS
alephzain
Vulnerability discovery and original root exploit
Tap to reach XDA discussion thread
supercurio
androidcentral

A new kernel exploit has been found (credit to *alephzain* at *XDA*) that affects some Samsung Exynos chipsets -- which happen to power many of Samsung's more popular phones. Normally kernel exploits don't make the rounds as news, but this time the word «malware» got attached to it so it has a bit of steam behind it.

Let's start this by reminding everyone that ***any app or program that roots your Android phone or jailbreaks your iOS device is malware by this definition***. People really need to give up on that damn click-bait, and instead worry about educating people to help keep them safer. That's what we're going to try to do, so read on and lets have a look.

Update: A couple new things here. First is that *Supercurio* has worked up a quick and easy app that'll patch this exploit if you're worried about it. It'll let you know if your device is vulnerable, closes the exploit without requiring root access (so it should work on any phone or tablet), and it «doesn't modify your system, copy files or flash anything.» You can turn the fix off and on as you choose, which is good because it breaks camera functionality on some devices (read more after the break on why that happens), and it could mess with HDMI output on some devices, Supercurio says. Also, we're re-emphasizing Chainfire's thread in the link below. Great stuff from the Android community. Let's hope Samsung gets something pushed out on its end as soon as it can.

Source: XDA; More: Chainfire's ExynosAbuse root exploit thread

The exploit and affected devices

The actual exploit itself only affects devices with the Exynos 4210 and 4412 processor. That means the Sprint Galaxy S II, the international Galaxy S II, the international Galaxy S3, the international Galaxy Note, and the Galaxy Note 2 are all affected, as well as tablets using the Exynos 4 -- certain Galaxy Player models, Galaxy Tab 2 devices and the Galaxy Note 10.1. We also don't want to forget the Galaxy Camera. While the U.S. versions of the Galaxy S3 are safe this time, that's still a whole lot of phones. There are also a few other phones (like the MEIZU MX) that use this SoC and may be affected.

Why is this different?

But why is what's basically a one-click root APK making the news? It's a pretty severe bug in Samsung's kernel source that lets users have access to the device RAM, and then we're free to dump it and see what's there or inject new processes of our own. The proof-of-concept APK that roots all the above named devices with one click (note that even the Verizon Galaxy Note 2 with a locked bootloader is easily rooted) is a perfect example. The train of thought is that an app could be built with this exploit hidden inside, rooting your phone without your knowledge.

http://www.androidcentral.com/samsung-exynos-kernel-exploit-what-you-need-know

The Samsung Exynos kernel exploit - what you need to know

It then could use the new elevated permissions to send data off to somewhere else, or do any number of equally dirty things you can do with root access. These apps could be distributed anywhere, and are easily installable. Always remember that a rooted phone or an unlocked bootloader means half the work for «the bad guys» is already done. This exploit makes that half easy for those same bad guys if your device is not rooted.

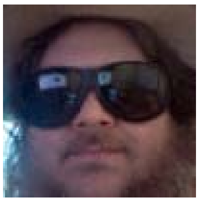
What should I do?

First, make sure your device is one that could be affected, We've listed them above, but if you still have questions ask in the forums. It's important to know if your device is affected or not. There are plenty of people who will give you the answer you're looking for.

If you're one of the many who have a custom ROM to help get away from the TouchWiz, you'll need to get with your ROM developer and see if that ROM's kernel is affected. Your device probably already is rooted, but you still don't want to be running around with a big unpatched hole that lets an app read a dump of your device memory.

If you're using a stock device and it's affected by this, your phone won't suddenly go rogue all on its own. You'll need to be mindful of what you're downloading and installing, especially if you're downloading and installing pirate copies of apps. (Which you should be mindful of anyway.) There is no specific app permission to look out for, as any app is able to access the device memory. You'll have to be vigilant -- just like you always should be. It's worth noting that nobody has seen or heard of any malware using this bug, and likely never will.

Samsung, here is your chance to make us love you even more. While this is not the «sky-is-falling» scenario that many will make it out to be, it is a critical flaw in the kernel that needs addressed quickly and thoroughly. We have no doubts that a patch will come soon that fixes the permissions, but having the patch and getting it to your users is another matter. We've reached out to Samsung for their side of this one, we'll let you know as soon as they respond.



- Related devices:
- Filed under:
- Tags: