Kernel Backdoor found in Gadgets Powered by Popular Chinese ARM Maker

By The Hacker News

Published: 2016-05-12 · Archived: 2026-04-05 16:29:47 UTC

How to Hack an Android device?

It is possibly one of the most frequently asked questions on the Internet.

Although it's not pretty simple to hack Android devices and gadgets, sometimes you just get lucky to find a backdoor access.

Thanks to Allwinner, a Chinese ARM system-on-a-chip maker, which has recently been caught shipping a version of Linux Kernel with an incredibly simple and easy-to-use built-in backdoor.

Chinese fabless semiconductor company Allwinner is a leading supplier of application processors that are used in many low-cost Android tablets, ARM-based PCs, set-top boxes, and other electronic devices worldwide.

Simple Backdoor Exploit to Hack Android Devices

All you need to do to gain root access of an affected Android device is…

Send the text "**rootmydevice**" to any undocumented debugging process.

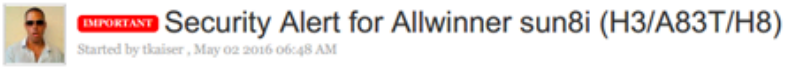
The local privileges escalation backdoor code for debugging ARM-powered Android devices managed to make its way in shipped firmware after firmware makers wrote their own kernel code underneath a custom Android build for their devices, though the mainstream kernel source is unaffected.

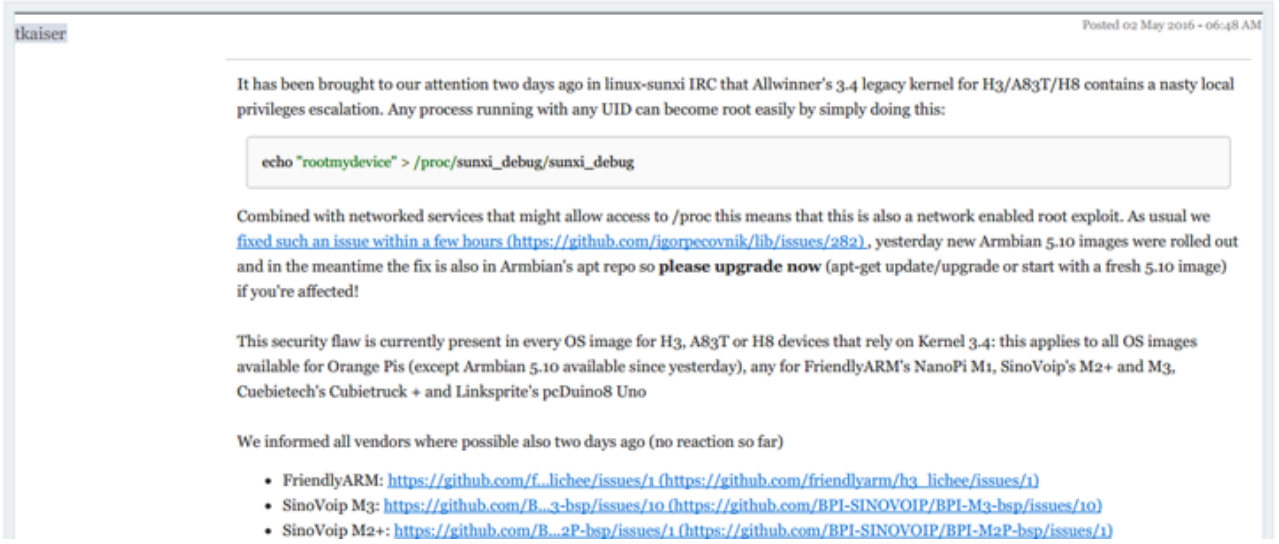
The backdoor code is believed to have been left by mistake by the authors after completing the debugging process.

For exploiting this issue, any process running with any UID can be converted into root easily by simply using the following command:

> **echo "rootmydevice" > /proc/sunxi_debug/sunxi_debug**

The *Linux 3.4-sunxi kernel* was originally designed to support the Android operating system on Allwinner ARM for tablets, but later it was used to port Linux to many Allwinner processors on boards like Banana Pi micro-PCs, Orange Pi, and other devices.




tkaiser

Posted 02 May 2016 - 06:48 AM

It has been brought to our attention two days ago in linux-sunxi IRC that Allwinner's 3.4 legacy kernel for H3/A83T/H8 contains a nasty local privileges escalation. Any process running with any UID can become root easily by simply doing this:

```
echo "rootmydevice" > /proc/sunxi_debug/sunxi_debug
```

Combined with networked services that might allow access to /proc this means that this is also a network enabled root exploit. As usual we fixed such an issue within a few hours (https://github.com/igorpecovnik/lib/issues/282), yesterday new Armbian 5.10 images were rolled out and in the meantime the fix is also in Armbian's apt repo so **please upgrade now** (apt-get update/upgrade or start with a fresh 5.10 image) if you're affected!

This security flaw is currently present in every OS image for H3, A83T or H8 devices that rely on Kernel 3.4: this applies to all OS images available for Orange Pis (except Armbian 5.10 available since yesterday), any for FriendlyARM's NanoPi M1, SinoVoip's M2+ and M3, Cuebietech's Cubietruck + and Linksprite's pcDuino8 Uno

We informed all vendors where possible also two days ago (no reaction so far)

- FriendlyARM: https://github.com/f...lichee/issues/1 (https://github.com/friendlyarm/h3_lichee/issues/1)
- SinoVoip M3: https://github.com/B...3-bsp/issues/10 (https://github.com/BPI-SINOVOIP/BPI-M3-bsp/issues/10)
- SinoVoip M2+: https://github.com/B...2P-bsp/issues/1 (https://github.com/BPI-SINOVOIP/BPI-M2P-bsp/issues/1)

At the forum of the Armbian operating system, a moderator who goes by the name Tkaiser noted that the backdoor code could remotely be exploitable *"if combined with networked services that might allow access to /proc."*

This security hole is currently present in every operating system image for A83T, H3 or H8 devices that rely on kernel 3.4, he added.

This blunder made by the company has been frustrating to many developers. Allwinner has also been less transparent about the backdoor code. David Manouchehri released the information about the backdoor through its own Github account (Pastebin) and then apparently deleted it.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
