SPC-21 · Mobile Threat Catalogue

Archived: 2026-04-05 21:54:57 UTC

Mobile Threat Catalogue

Low-level Backdoor

Contribute

Threat Category: Supply Chain

ID: SPC-21

Threat Description: Low level backdoor inadvertently left by firmware developer.

Threat Origin

This is what a root debug backdoor in a Linux kernel looks like [1]

Chinese ARM vendor left developer backdoor in kernel for Android, other devices [2]

Exploit Examples

Not Applicable

CVE Examples

Not Applicable

Possible Countermeasures

Enterprises

Obtain devices from a reputable vendor with a strong record of addressing security flaws in a timely fashion.

Mobile Device User

Obtain devices from a reputable vendor with a strong record of addressing security flaws in a timely fashion.

To reduce the opportunity for an attacker to exploit a patched vulnerability, ensure security updates are applied in a timely manner by configuring automated installation of or, at a minimum, automatic notification of the availability of security updates.

To reduce the opportunity for attacks against various firmware components, disable device features when not in use (e.g., Bluetooth, Wi-Fi, NFC), and globally revoke access to unused device sensors or OS-provided functions (e.g., camera, microphone, location services).

Enterprise

To reduce the opportunity for an attacker to exploit a patched vulnerability, ensure security updates are applied in a timely manner by configuring automated installation of or, at a minimum, automatic notification of the availability of security updates.

References

1. R. Chirgwin, “This is what a root debug backdoor in a Linux kernel looks like,” The Register, 9 May 2016; http://www.theregister.co.uk/2016/05/09/allwinners_allloser_custom_kernel_has_a_nasty_root_backdoor/ ↩

2. S. Gallagher, “Chinese ARM vendor left developer backdoor in kernel for Android, other devices,” Ars Technica, 11 May 2016; http://arstechnica.com/security/2016/05/chinese-arm-vendor-left-developer-backdoor-in-kernel-for-android-pi-devices/ ↩
