Android crypto key vulnerability affects only 10 percent handsets: report

June 30 2014, by Nancy Owano

IBM researchers have called attention to a serious Android crypto key theft vulnerability but the vulnerability affects only version 4.3, which runs on about 10.3 percent of handsets, reports Dan Goodin in *Ars Technica*, in a June 30 update of his report. IBM researchers had shed light on the vulnerability, which may allow attackers to steal credentials,

including cryptographic keys for banking services and virtual private networks, and PINs or patterns to unlock vulnerable devices. Pau Oliva, senior mobile security engineer at viaForensics, said in Ars Technica that a malicious user exploiting this vulnerability would be able to do RSA key generation, signing, and verification on behalf of the smartphone owner. The bug resides in Android KeyStore, said Goodin. This is the sensitive region of the operating system dedicated to storing cryptographic keys and similar credentials, according to the security advisory posted by Roee Hay, who leads the application security research team at IBM.

The IBM report detailed the impact that an exploit could have. "Successfully exploiting this vulnerability leads to a malicious code execution under the keystore process." Such code can leak the device's lock credentials, leak decrypted master keys, data and hardware-backed key identifiers from the memory. leak encrypted master keys, data and hardware-backed key identifiers from the disk for an offline attack, interact with the hardware-backed storage, and perform crypto-operations such as arbitrary data signing on behalf of the user. Android 4.4, however, is not vulnerable; Android has patched KitKat. On June 23 the discovery by IBM was publicly disclosed, after they had reported the vulnerability in September last year to the Android Security Team. In response the Android team acknowledged the vulnerability and in November last year the fix was confirmed.

In Hay's June 30 update, he thanked the Android Security Team and he explained why the IBM team waited before making the public disclosure in June this year.

"Nine months ago, my team came across a classic stack-based buffer overflow in the Android KeyStore service. As always, we adhered to our responsible disclosure policy and privately reported this issue to the Android Security Team; the result is a patch that is now available in

KitKat. Considering Android's fragmented nature and the fact that this was a code-execution vulnerability, we decided to wait a bit with the public disclosure."

A list of what's new for developers in Android 4.4 KitKat includes a section on security enhancements. According to the site, among the enhancements are improved cryptographic algorithms. "Android has improved its security further by adding support for two more cryptographic algorithms. Elliptic Curve Digital Signature Algorithm (ECDSA) support has been added to the keystore provider improving security of digital signing, applicable to scenarios such as signing of an application or a data connection. The Scrypt key derivation function is implemented to protect the cryptographic keys used for full-disk encryption."

More information: arstechnica.com/security/2014/ … fects-86-of-devices/