Security CTO to detail Android Fake ID flaw at Black Hat

July 29 2014, by Nancy Owano

Where have you heard this before: A team of security researchers discover a security flaw in Android devices. This is, however, news. This time, experts are talking about a flaw that involves a widespread vulnerability dating back to the release of Android 2.1.

Bluebox Labs claims that Fake ID has been present in Android from version 2.1, leaving a substantial number of devices running earlier versions of the operating system vulnerable. Reports say the flaw involves devices still running Android 2.1 to Android 4.3, with affected users potentially left open to attack from malicious apps that would

appear to come from legitimate developers. The Android vulnerability, dubbed Fake ID, can enable malware to impersonate trusted applications. The vulnerability was posted in a blog Tuesday by Bluebox Security CTO Jeff Forristal, based on research by the company's Bluebox Labs. They found identities can be copied. How much mischief can be done? He said, "the vulnerability can be used by malware to escape the normal application sandbox and take one or more malicious actions: insert a Trojan horse into an application by impersonating Adobe Systems; gain access to NFC financial and payment data by impersonating Google Wallet; or take full management control of the entire device by impersonating 3LM."

The team found that Fake ID is the result of how Android checks app security, with each app given a cryptographic signature determining who can update it, and what privileges it has. Bluebox said up until KitKat, Android did not carry out adequate checks on the certificate chain. Forrestal told the BBC, "That missing link of confirmation is really where this problem stems." Forristal said it was like a tradesman entering a building and showing his ID to a security guard and being given special access without any phone call made to the tradesman's employer to check if the person is really on the books.."The fundamental problem," he added, "is simply that Android doesn't verify any claims regarding if one identity is related to another identity."

Gizmodo noted that a patch was issued by Google to Android partners and to the Android Open Source Project. The Guardian on Tuesday said Google has not seen evidence of attempted exploitation of this vulnerability. The Guardian quoted a Google spokesperson: "Google Play and Verify Apps have also been enhanced to protect users from this issue. At this time, we have scanned all applications submitted to Google Play as well as those Google has reviewed from outside of Google Play and we have seen no evidence of attempted exploitation of this vulnerability." According to the BBC, a Google spokesperson also said,

"We appreciate Bluebox responsibly reporting this vulnerability to us. Third-party research is one of the ways Android is made stronger for users."

Forristal will speak about this next week at the Black Hat Security event in Las Vegas. He said his talk will cover technical details, where he will review the bug, including how it was found, and how it works.

More information: www.blackhat.com/us-14/briefin … rability-walkthrough
bluebox.com/technical/android- … ake-id-vulnerability