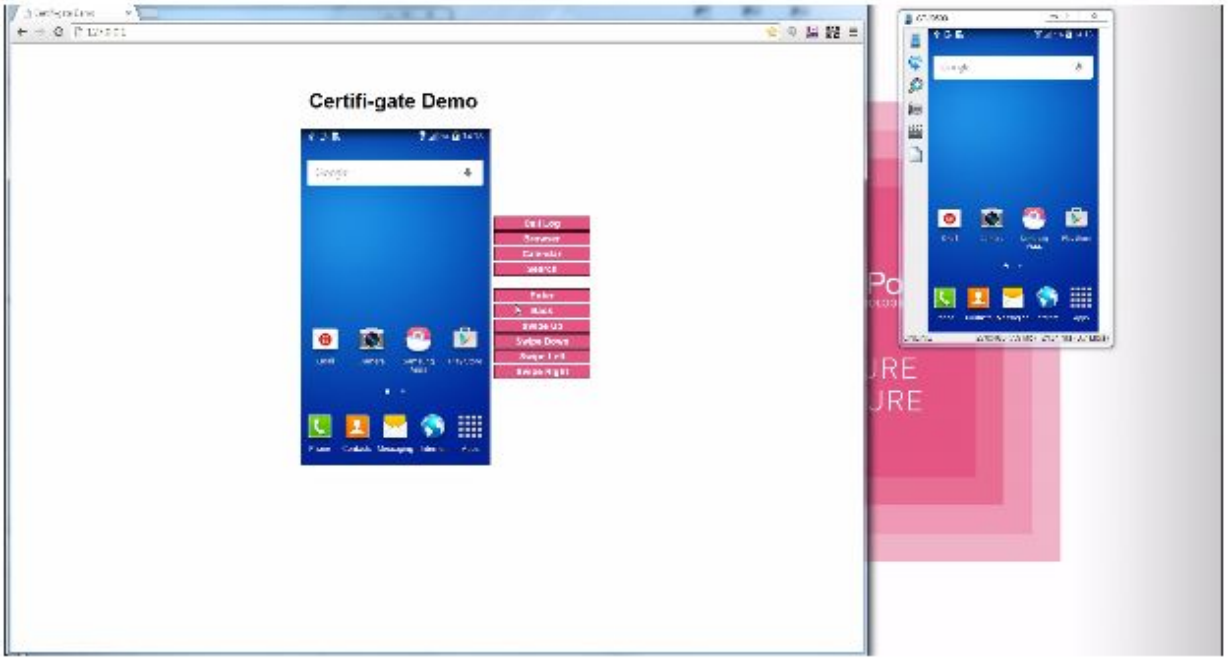
Android uh-oh resides in vulnerability dubbed Certifi-gate

August 7 2015, by Nancy Owano



An Android vulnerability has been discovered which leaves phones at risk of malicious apps gaining privileged access without a victim being aware of all this. The weakness affects phones from a number of major manufacturers. The vulnerability on such phones involves even those running the latest version of Android.

Researchers who explored the flaw are from the security company Check Point, and they are calling it "Certifi-gate." They said the vulnerability can be used by cyberthieves to steal sensitive data. They disclosed their findings at a briefing session at Black Hat USA 2015 in Las Vegas.

Users cannot disable anything that will fix the problem, which involves software that was installed by the manufacturers themselves. This software is what thieves could exploit in order to gain privileged access. James Titcomb in *The Telegraph* said, "Phone manufacturers install plugins on smartphones before they are sold that allow them, or a network operator, to remotely access the phone using remote support tools." Malware can masquerade as one of these tools with the use of fake security certificates, gaining control.

Adam Clark Estes in *Gizmodo* similarly said: "The apps in question are known as mobile remote support tools (mSRTs). These often come pre-installed by the manufacturer or carrier and enable support teams to access and control devices remotely, mainly for fixing problems."

The good news: A number of manufacturers have issued updates to address the issue.

The Register said affected vendors were notified by Check Point about Certifi-gate and have begun releasing updates. *Gizmodo* said the Check Point team reported the vulnerability to Google, a number of device manufacturers and carriers; many already addressed it.

Senior Editor Roberto Baldwin, *Engadget*, carried Samsung's response: "At Samsung, we understand that our success depends on consumers' trust in us, and the products and services that we provide. We are aware of Check Point's alleged claims, and Samsung has addressed this issue. Samsung encourages users not to execute unsecure apps."

A Google spokesperson commented, according to several sites: "We want to thank the researcher for identifying the issue and flagging it for us. The issue they've detailed pertains to customizations Original Equipment Manufacturers make to Android devices and they are providing updates which resolve the issue. Nexus devices are not affected and we haven't seen attempts to exploit this."

Google offered advice: "We strongly encourage users to install applications from a trusted source, such as Google Play."

Meanwhile, Check Point offered a link where one can download their Certifi-gate report. They also made a scanner available so that visitors can see if they are vulnerable to the flaw.

More information: blog.checkpoint.com/2015/08/06/certifigate/

Citation: Android uh-oh resides in vulnerability dubbed Certifi-gate (2015, August 7) retrieved 19 April 2024 from https://techxplore.com/news/2015-08-android-uh-oh-resides-vulnerability-dubbed.html