New Android Installer Highjacking Vulnerability Exposes Android Device Users to Data Theft and Malware

March 24, 2015

Vulnerability Affects Users Downloading Android Applications from Third-party Sources

SANTA CLARA, Calif., March 24, 2015 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), the leader in enterprise security, today revealed details of a widespread vulnerability in Google's Android mobile operating system that allows attackers to hijack the installation of a seemingly safe Android application -- Android Package File (APK) -- on user devices, and replace it with an app of the attacker's choice, without user knowledge.

Exploitation of this vulnerability, which is estimated to affect about 49.5 percent of current Android device users, allows attackers to potentially distribute malware, compromise devices and steal user data. Palo Alto Networks today also released an application to help potentially affected Android users diagnose their devices.

Vulnerability Allows Stealth Bait & Switch
Discovered by Palo Alto Networks Unit 42 threat researcher Zhi Xu, the vulnerability exploits a flaw in Android's "PackageInstaller" system service, allowing attackers to silently gain unlimited permissions in compromised devices. Specifically:

- During installation, Android applications list the permissions requested to perform their function, such as a messaging app requesting access to SMS messages, but not GPS location.
- This vulnerability allows attackers to trick users by displaying a false, more limited set of permissions, while potentially gaining full access to the services and data on the user's device, including personal information and passwords.
- While users believe they are installing a flashlight app, or a mobile game, with a well-defined and limited set of permissions, they are actually running potentially dangerous malware.

Unit 42, the Palo Alto Networks threat intelligence team, has worked with Google and Android device manufacturers such as Samsung and Amazon to help protect users and patch this vulnerability in affected versions of Android. Some older-version Android devices may remain vulnerable.

QUOTE:

- "This Android vulnerability means users who think they're accessing legitimate applications with approved permissions may instead be exposed to data theft and malware. We urge users to take advantage of the diagnostic application provided by Palo Alto Networks to check their devices, and we thank Google, Samsung and Amazon for their cooperation and attention."
  – Ryan Olson, Intelligence Director, Unit 42, Palo Alto Networks

Mitigation
The vulnerability disclosed today affects Android applications downloaded from third-party sources, and does not affect applications accessed from Google Play. Palo Alto Networks recommends the following for enterprises concerned about the risk of malware through Android devices:

- On vulnerable devices, only install software applications from Google Play; these files are downloaded into a protected space, which cannot be overwritten by the attacker.
- Deploy mobile devices with Android 4.3_r0.9 and later, but keep in mind that some Android 4.3 devices are found to be vulnerable.
- Do not provide apps with permission to access logcat. Logcat is a system log, which can be used to simplify and automate the exploit. Android 4.1 and later versions of Android by default forbid apps from accessing logcat of system and other installed apps. But an installed app could still manage to get access to other apps' logcat on rooted mobile devices using Android 4.1 or later.
- Do not allow enterprise users to use rooted devices with enterprise networks.

To learn more

- Read full details of this Android vulnerability on the Unit 42 blog, and subscribe to regular research and analysis updates: http://researchcenter.paloaltonetworks.com/2015/03/android-installer-hijacking-vulnerability-could-expose-android-users-to-malware/
- Watch a short video describing Android Installer Hijacking to understand which Android devices are vulnerable and why: http://youtu.be/81slOhjrZXY
- Download the scanner application:
  - Via GitHub: https://github.com/PaloAltoNetworks-BD/InstallerHijackingVulnerabilityScanner

    - Via Google Play: http://play.google.com/store/apps/details?id=com.paloaltonetworks.ctd.ihscanner
- Visit the Unit 42 homepage for new research, updates and confirmed speaking appearances: https://www.paloaltonetworks.com/threat-research.html
- Learn more about Palo Alto Networks enterprise security platform: https://www.paloaltonetworks.com/products/platforms.html
- Meet Unit 42 team leads at Ignite 2015, where your toughest security challenges get solved. Register now to join us next week in Las Vegas, March 30-April 1, 2015.

About Unit 42
Unit 42, the Palo Alto Networks threat intelligence team, is made up of accomplished cybersecurity researchers, and industry experts. Unit 42 gathers, researches, and analyzes up-to-the-minute threat intelligence, sharing insights with Palo Alto Networks customers, partners, and the broader community to better protect organizations. Unit 42 team leads regularly appear at industry conferences throughout the world.

About Palo Alto Networks
Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government, and service provider networks from cyber threats. Unlike fragmented legacy products, our security platform safely enables business operations and delivers protection based on what matters most in today's dynamic computing environments: applications, users, and content. Find out more at www.paloaltonetworks.com.

Logo - http://photos.prnewswire.com/prnh/20130508/SF04701LOGO

To view the original version on PR Newswire, visit:http://www.prnewswire.com/news-releases/new-android-installer-highjacking-vulnerability-exposes-android-device-users-to-data-theft-and-malware-300054515.html

SOURCE Palo Alto Networks

Jennifer Jasper-Smith, Head of Corporate Communications, Palo Alto Networks, 408-638-3280, jjsmith@paloaltonetworks.com; Tim Whitman, Voce Communications, 617-721-5994, twhitman@vocecomm.com