

ZTE scrambles to get at root of phone flaw

May 18 2012, by Nancy Owano



The ZTE Score M

(Phys.org) -- Rattling phone security news surfaced this week for those owning ZTE Score M phones after an anonymous post to Pastebin.com reported a backdoor hole where others can gain control over a user's device. The hole allows anyone with hardwired password to access the affected phone. ZTE has reacted in the affirmative, acknowledging the vulnerability in the Score phone and saying they're working on a security patch, which it will issue soon. "We strongly urge affected users to download and install the patch as soon as it is rolled out to their devices."

As the world's number-four handset vendor, ZTE Corp. and another Chinese equipment maker Huawei Technologies have been subjects of a

controversy over whether their expanded presence in a U.S. market poses security risks from feared backdoors. Recently, a U.S. congressional panel singled out Huawei and ZTE in approving a measure designed to search and clear the U.S. nuclear-weapons complex of any technology produced by the two companies.

ZTE issued ZTE Score M as an affordable Android phone, the ZTE Score M. with a 3.5-inch HVGA touchscreen, 600MHz CPU, 3.2-megapixel camera, Wi-Fi, and microSD slot. Unfortunately, news surfaced that it also had the unwelcome feature of a root backdoor. The setuid-root binary, a program that runs with root privileges in /system/bin/sync_agent, provides the backdoor. Anyone who knows the hard-coded password gets root access to the phone.

ZTE could have used the backdoor as a way for ZTE to update the phone's software. Security experts say it is not clear whether ZTE is a victim of sloppy programming or whether this had worse intent.

Dmitri Alperovitch, co-founder of cybersecurity firm, CrowdStrike and former Vice President of Threat Research at McAfee, noted that it is rare to find a vulnerability apparently inserted by the hardware manufacturer.

There are conflicting reports over whether the hole affects other ZTE phones. ZTE confirmed the vulnerability on its Score [phone](#) but has denied that it affected other models as well. Nevertheless, some reports said ZTE Skate phones, sold by Orange in the UK, has the same backdoor. According to reports, security researchers are working to see if other ZTE devices suffer from the same [security](#) vulnerability.

In Australia, [ZTE](#), with offices in Sydney and Melbourne, supplies some Telstra phones. They are typically rebranded as T- and F-series mobile phones. Telstra, according to reports, knew about the backdoor news and

was testing its devices, but preliminary tests looking for backdoor flaws suggested its handsets were not affected.

© 2012 Phys.Org

Citation: ZTE scrambles to get at root of phone flaw (2012, May 18) retrieved 13 May 2024 from <https://phys.org/news/2012-05-zte-scrambles-root-flaw.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.