

Google G1 Phone: Security Flaw Exposed

October 28 2008, by John Messina



(PhysOrg.com) -- A group of Security Researchers exposed a security flaw in Google's G1 Android phone. The flaw is in the web browser on the T-Mobile G1 that can potentially allow Trojans and Keyloggers to install themselves on your phone if you visit a website with malicious code.

Android, Google's open source software is based on outdated open-source components which had known vulnerabilities and were fixed. Google admitted that they did not incorporate the security fixes into

Android.

For Google's G1 phone to become infected, a malicious developer would need to know what the flaw is and then needs to place this malicious code on a website. Unless you are searching for suspicious websites that may be affected, the chances are good that you are safe from infection.

Google said it is developing a solution to the problem. "We are working with T-Mobile to include a fix for the browser exploit, which will soon be delivered over the air to all devices, and have addressed this in the Android open-source platform.

This incident raises concerns about potential difficulties that the Android community might face in the future. Because Google has adopted an open model with Android, many vendors and operators in the future may offer a variety of phones. If vulnerabilities are found in the future, phone makers and operators will have to determine if their version of the software is affected and then coordinate the distribution of a fix to all users.

Citation: Google G1 Phone: Security Flaw Exposed (2008, October 28) retrieved 21 September 2024 from <https://phys.org/news/2008-10-google-g1-flaw-exposed.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.