Chrome for Android vulnerability discovered by researcher

November 13 2015, by Nancy Owano

Making news this week at the MobilePwn2Own event at the PacSec conference in Tokyo: an exploit of Google's Chrome for Android—in one shot, said PacSec organizer Dragos Ruiu. Researcher Guang Gong showcased the exploit. (PacSec is a computer security event. James O'Malley in *TechRadar* described it as "a meeting of security experts who show off what they've discovered for the kudos.")

Ruiu talked to *Vulture South*, the Asia-Pacific bureau based in Sydney of *The Register*. He told Vulture South the exploit was demonstrated on a

Google Project Fi Nexus 6. The exploit targets the JavaScript v8 engine and was notable, said the report, as "a single clean exploit that does not require multiple chained vulnerabilities to work."

While the exploit was not disclosed in full detail, Ruiu described the results in *The Register*. As soon as the phone accessed the website, the JavaScript v8 vulnerability in Chrome was used to install an arbitrary application, without user interaction, to demonstrate control of the phone. In theory, it would translate into unauthorized code running on a person's phone.

V8 is Google's open source JavaScript engine. V8 is written in C++ and is used in Google Chrome, the open source browser from Google.

A Google security engineer on site received the bug. *Softpedia* stated that "A Google engineer immediately got in contact with Gong after his presentation, and rumors have it that the Chrome team is already getting a fix ready."

(Not responding specifically to this event but relevant, the HackerOne blog recently observed how "data show that programs that respond quickly to new reports, and keep open communication channels during the triage and resolution process, tend to get more reports and more repeat researchers, leading to a virtuous, security-enhancing cycle. In addition, the timely resolution of vulnerabilities reduces the risk of potential exploitation, leading to greater security.")

Gong is a security researcher at Qihoo 360. "Thankfully," commented *9to5Google*, "the exploit was developed by someone whose job it is to find vulnerabilities, and not a hacker with malicious intent."

Ruiu will fly Gong to the CanSecWest security conference next year, said *The Register*.

The Android security team recognizes those who help to improve Android security by responsibly reporting vulnerabilities or by committing code with positive impact on Android security.

In the bigger picture, *Fortune* senior writer Barb Darrow observed that "Given the high interest level in hacking and growing intensity of security breaches, there is definitely a need for legitimate hackers to test the limits of software."

Gong said it took him three months of work prior to the competition to find the hole, according to *Business Insider Australia*.

"Good news here is that since it's through Chrome, we don't need to wait for an OTA to be approved by the manufacturers, and then the carriers," said *Android Headlines* on Friday.