Hacker group finds a way to gain root access to Chromecast

July 29 2013, by Bob Yirka

(Phys.org) —GTVHacker has [posted](#) a blog entry describing a hack they've done on Google's new streaming stick Chromecast. Because the process is so simple, it appears as if Google intentionally left the "vulnerability" open for hackers and other commercial enterprises to exploit, much as they have done with Android devices.

Chromecast is a small (flash drive sized) device that connects directly to a television's HDMI port. Once installed it allows for wirelessly [streaming content](#) from a computer or handheld device to the [television set](#). Principle streaming sources include Netflix and YouTube. The

introduction of Chromecast created quite a stir when it was released last week as its price is a mere $35. As has been the case with virtually every other hardware device released to the public, hackers appear to have set to work trying to gain access to control the device in ways not intended by the manufacturer.

GTVHacker notes that the OS on the device is not Chrome (as its name implies) but a stripped down version of the software used to run Google TV. To gain access, a [flash drive](#) was attached to the device and then the power on/off button was held down (causing it to boot to USB mode) as the device was being powered on. Natural code on the device calls for a signed image to be detected on the USB device. As no verification of the image was required, the hackers were able to execute other code that they had written. Specifically, their hack allows for spawning a root shell on port 23.

That a hacker team was able to find such a vulnerability and exploit it in just four days is likely no surprise to Google. They've been using the services of hacker groups to help test new products since the introduction of Gmail and Android—doing so led to the early development of smartphone apps, and Google is no doubt hoping the same thing happens with Chromecast—early reports suggest its native applications are severely limited. The hack found by the team at GTVHacker means that pretty much anyone that wishes can development custom apps for the device, perhaps making it worth far more than its list price.

© 2013 Phys.org