Some HTC Android phones found vulnerable to WiFi password leak

February 2 2012, by Bob Yirka

HTC Desire HD

(PhysOrg.com) -- The United States Computer Emergency Readiness Team (U-CERT) has issued a warning to users of some HTC Android phones regarding a security vulnerability that has been found. The warning pertains to 802.1X WiFi user information and SSID data that can be viewed by rouge applications, taking advantage of a weakness in the OEM Android build of certain HTC phones.

Affected phones allow 802.1X WiFi information to be seen by applications that have access rights to WiFi information stored on the phone. This means errant applications could find their way to a stored SSID (Service Set Identifier - an identifier attached to the header of packets sent to a wide area network), login names as well as passwords.

Also, should the phone connect to the Internet, identified information could then be sent back to those that created the application and who are looking for such information. And if the phone also connects to a corporate network, the vulnerability could lead to data being stolen.

According to U-CERT, the phones at risk are:

Desire HD (both "ace" and "spade" board revisions) - Versions FRG83D, GRI40
Glacier - Version FRG83
Droid Incredible - Version FRF91
Thunderbolt 4G - Version FRG83D
Sensation Z710e - Version GRI40
Sensation 4G - Version GRI40
Desire S - Version GRI40
EVO 3D - Version GRI40
EVO 4G - Version GRI40

HTC, a Taiwanese manufacturer of Smartphones, has had other security issues with their phones in just the past few months, and according to some unofficial sources, this particular vulnerability was discovered by Chris Hessing, a senior engineer with CloudPath Networks. Google and HTC were both apparently notified about the vulnerability last September after it was discovered. Since that time, both have been hard at creating a fix, which is now available to worried owners at HTC's support site.

Google has also reportedly performed a full scan on all of the applications available for download in the Market, and has found none that have tried to take advantage of the vulnerability, indicating that it's possible nobody but Hessing and workers at HTC and Google were even aware of the vulnerability, which means despite the lapse by HTC, it's likely no one was actually harmed by the problem.