QR code security vulnerability found with Google Glass

July 18 2013, by Bob Yirka

Engineers at Lookout Mobile Security have discovered a previously unknown security vulnerability with Google's project Glass wearable headset. Marc Rogers reports on the company's web site that engineers found that when pictures were taken of printed QR codes, the device could be routed to a hostile Wi-Fi access point, which in turn allowed for monitoring and capture of data flow to and from the device. They also found they were able to divert the device to a web page that allowed for taking advantage of a previously known Android vulnerability.

Google Glass, Google's augmented reality headset runs Android, and because of that is able to run many of the same apps as smartphones, one of which allows for reading, recognizing and responding to QR codes. Such codes have been designed for that very purpose. In testing the feature with a Glass device, the engineers at Lookout Mobile Security found that they could cause the device to connect to the Internet using a previously rigged Wi-Fi hotspot. In so doing, they found they were able to monitor traffic between the device and the Internet, picking up message content and images that were transferred. They also found that they could cause the device to be routed to a web page they'd set up that allowed them to take control of the device using a previously known Android vulnerability. That allowed them to read messages stored on the device, control the camera and perform any other phone function.

Rogers told the press that Google was notified of the vulnerability on May 16th and that the company has taken steps to head off the problem. A subsequent software update by Google shows that code has been amended to prevent the automatic relocation of a Wi-Fi hotspot when reading a QR code. Users are now asked if they wish to switch over.

In response to publication of the discovery of the vulnerability, Google representatives reminded the press that Glass is still in a testing phase. Giving demo units to select users allows for finding and fixing vulnerabilities, they noted, as well as for spotting bugs or user issues before the device is made available to the general public.