theguardian

Google Glass hacked with malicious QR code to yield its pictures and video

Lookout Security discovers flaw in early software on Google head-mounted system which lets it take control of data coming from wearable system

Charles Arthur
guardian.co.uk, Wednesday 17 July 2013 07.18 EDT

George Prentzas's Darth Vader QR code cross stitch: this one is safe, but a malicious QR code hacked older Google Glass software Photograph: George Prentzas

Researchers at mobile security company Lookout discovered a security flaw in Google Glass which allowed them to capture data being sent from the head-mounted device to the web without the user's knowledge.

The flaw used the fact that the head-mounted Glass camera scans any photo it takes for a QR code in order to set up Wi-Fi or Bluetooth connections to a smartphone for internet access.

Whenever the Glass software detects a QR code, it decodes it to see if it names a Wi-Fi network to connect to. It will do this even if the code does not occupy the whole of the frame - so a hacker could get a Glass owner to hack their own device just by standing near a printout of special QR code.

"We created a QR code that told Glass to connect to a Wi-Fi network of my choosing and started sending data to that," Marc Rogers, principal security analyst at Lookout, told the Guardian. "We could become the middleman, and if we needed to strip out the encryption on the connection. Then we could see the pictures or video that it's uploading. We could also direct it to a site on the web which exploits a known vulnerability in Android 4.0.4" - used by Glass - "which hacked Glass at it browsed the page."

Rogers says that he discovered the flaw - which was disclosed to Google, and has since been fixed by a software update - on 17 May after about a week of experimentation. "I tried to work out where it was different from its parent smartphone," he said.

At Lookout, Rogers has blogged about the attack, pointing out that as the "internet of things" - connected devices - becomes larger and more prevalent, unexpected vulnerabilities may appear which would not be predictable through standard analysis.

Lookout has also confirmed the existence of a serious vulnerability in Android potentially affecting 99% of smartphones running the system, which was reported by Bluebox Security, a security startup based in San Francisco. Bluebox said that there is a "master key" which would let hackers modify the code of a downloadable app to turn it into a Trojan while retaining its old cryptographic signature on the Play store.

Though Google has taken measures to prevent that, Lookout has confirmed the flaw's existence and is rolling out a fix for customers using it software.

The Google Glass vulnerability meanwhile points to a new challenge as "connected devices" become more widespread - especially if, like Glass, they lack standard input systems such as keypads and so must rely on image recognition for control.

"Both the vulnerablity, and the way it was delivered, are unique to Glass - a consequence of it being connected," Rogers said. "I don't think anyone's hacked a device with an image before."

Google updated the flaw two weeks after being told about it, Rogers said.

Asked whether he thought there would be other flaws discovered in Glass, he said: "Every piece of software and hardware has flaws. What's particularly impressive is that Google realised there's a limited

subset of people capable of finding these bugs, and has seeded Glass to them before releasing it to consumers." That means that the most obvious security flaws should be discovered before consumers use them, he suggested.

But he said that he was "absolutely" sure more flaws would be found: "I'm looking forward to looking for more bugs." He wouldn't say whether Lookout had found more security flaws in the two months since reporting the QR code flaw to Google.

Google said in a statement: "We want get Glass into the hands of all sorts of people, listen to their feedback, see the inspirational ways they use the technology, and discover vulnerabilities that we can research and work to address before we launch Glass more broadly."

;