TechXplore

# Security experts reveal weakness in WiFi connected LIFX light bulbs

July 9 2014, by Bob Yirka

Experts at Context Security have announced that they found a security issue with LIFX smart-light bulbs. In hacking the firmware they found they were able to intercept messages sent across the mesh network, giving them access to WiFi passwords. After notification by Context, LIFX posted a notice to its web site acknowledging the security flaw and announcing that a security fix had been created and made available as part of a firmware update for their smart bulbs.

The report from Context highlights a growing security concern—devices that are part of the movement towards "The Internet of Things," where common devices such as refrigerators and lights are connected to the Internet allowing for remote control from phones, tablets or computers, may not be as secure as phones or computers. Hackers purchasing such products and finding security flaws in their firmware may be able to use what they learn to hack their way into private WiFi networks, and from there, user device data. There is also the issue of user involvement—it's doubtful that most people will go to the trouble of keeping up to date on firmware upgrades to fix security issues for devices in their homes that they rarely even think about.

The LIFX smart-bulb made news two years ago as a Kickstarter project—its developers collected over thirteen times the $100,000 they were looking for. The now established company competes with other smart-bulb products such as Philips Hue lights and GE's Link bulb.

Context experts purchased several of the LIFX smart-bulbs (LED bulbs connected to a WiFi enabled circuit board). They found that when the bulbs "talked" to each other across a (6LoWPAN powered) mesh network, the messages contained a username and password. Because the underlying pre-shared key was never changed, all the white-hat guys had to do to gain access was set up a similar circuit board simulating one of the smart bulbs asking to join the network. That allowed them to steal credentials and eventually gain control of all the lights on the network. They report that a potential hacker could have gained access in private homes or businesses if they could have gotten as close as 30 meters to the bulbs. They note also that such a hack would have gone undetected by the owner of the network.

**More information:** blog.lifx.co/

Citation: Security experts reveal weakness in WiFi connected LIFX light bulbs (2014, July 9) retrieved 19 April 2024 from https://techxplore.com/news/2014-07-experts-reveal-weakness-wifi-lifx.html