Now a smart lightbulb system got hacked

5 February 2020, by Jefferson Graham, Usa Today

That shiny new smart light bulb that can be turned on and off with Alexa and change colors with the Google Assistant could be vulnerable to a hack.

Security researchers from Check Point tested the Philips Hue models, the most popular smart lights brand, and says it successfully hacked into a home's computer network. It went to Philips to show its findings and says Philips has now fixed the issue, but Yaniv Balmas, Head of Cyber Research at Check Point Research says consumers of off-brand lights may not be as lucky.

Amazon lists many brands in its smart light offerings, including Philips, Wyze, Teckin and Berennis.

Balmas warns that the same protocol flaw found in the Hue bulbs is also used by other popular devices, including the Amazon Echo speakers and Belkin's WEMO.

The hack would enable someone to "gain entry and spread malware," into a home or office computer network easily, says Balmas.

If you connect anything that's smart, it comes with risks.

"We chose Philips because it has the biggest market share," in smart lights, says Balmas. "But if we found this in Philips, think about the vulnerabilities in other devices. Think of other bulbs and how many are made in China, with lower manufacturing costs. Would they be a much easier target to find vulnerabilities?"

The news follows months of reports of other digital products easily being hacked, from Ring video doorbells to self-driving cars.

What's a consumer to do to protect themselves? Start by updating software, be on the alert for out of the ordinary behavior of devices and separate the devices from others in the network on your router.

Many newer home routers let consumers create separate segments on the network, adds Balmas. This would get your light bulb off of the same network used for running your computer, and thus, the hacker wouldn't be able to get into your system, just your bulbs. The Linksys Mesh WiFi Router AC2200 ($157) for instance, says it can separate products on three different networks.

When informed of the hack by Check Point, Philips updated its protocols, which touted the safer Hue system in a Check Point release.

"We are committed to protecting our users' privacy and do everything to make our products safe. We are thankful for responsible disclosure and collaboration from Check Point It has allowed us to develop and deploy the necessary patches to avoid any consumers being put at risk," said George Yianni, Head of Technology for Philips Hue.

U.S. TODAY reached out to Amazon and WEMO. Amazon said, in a statement, "Customer trust is important to us and we take the security of our devices seriously. We are reviewing this research to determine if there is any impact on our devices,"

while WEMO didn't comment.

APA citation: Now a smart lightbulb system got hacked (2020, February 5) retrieved 19 October 2021 from https://techxplore.com/news/2020-02-smart-lightbulb-hacked.html