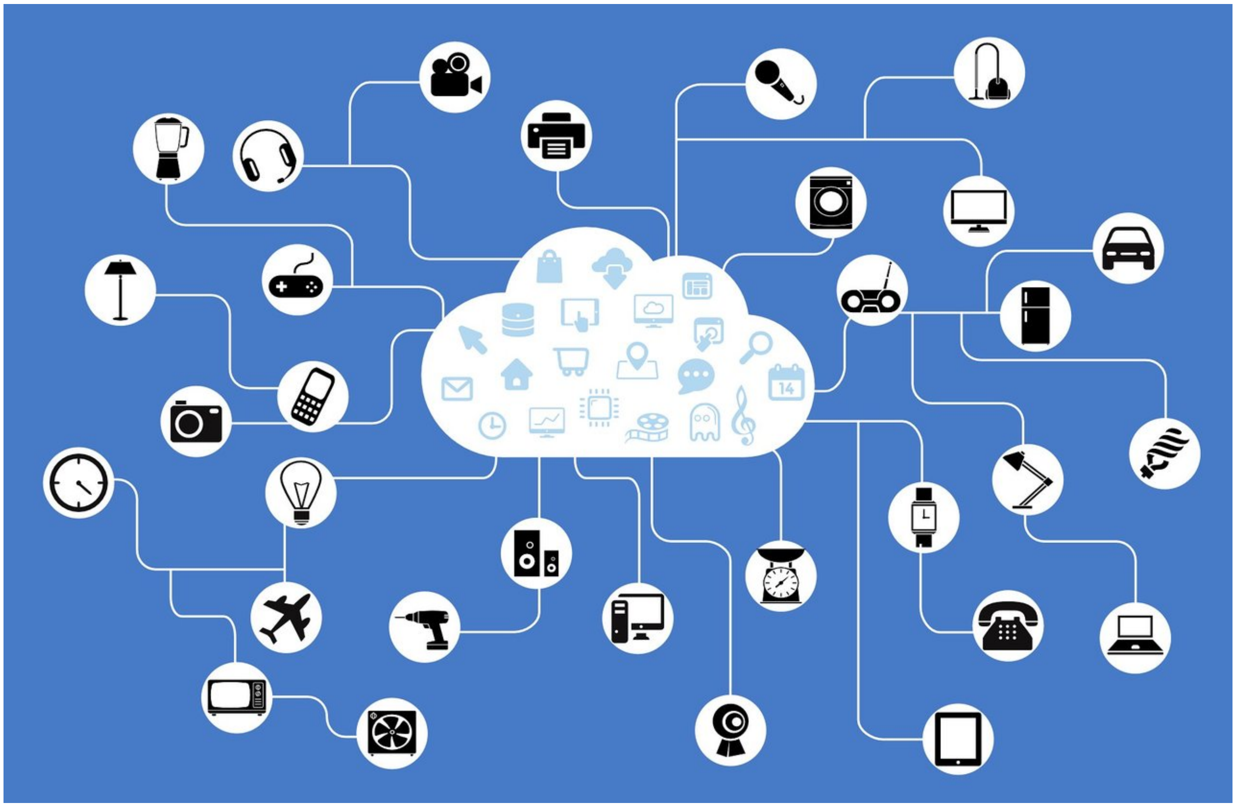
Vulnerability found in IoT devices that use ThroughTek 'Kalay' network

August 18 2021, by Bob Yirka



Credit: CC0 Public Domain

A team of researchers at Mandiant has found a security vulnerability in IoT devices that use the ThroughTek "Kalay" network. Parent company Fireeye has published a blog account of the work done by the team that discovered the threat, which explains how users can protect themselves.

ThroughTek has also posted a warning about the vulnerability on its website.

In working with a team at the Cybersecurity and Infrastructure Security Agency (CISA)—which has also posted an advisory, warning users of the vulnerability on its website—the team at Mandiant found that users of certain Internet of Things (IoT) devices could be at risk of having their privacy invaded. The researchers found that the vulnerability allowed potential hackers to access devices and to take control over them. This means that hackers could be listening in to conversations occurring near baby monitors, or nanny cameras, for example, or watching live video streaming from security cameras. The team at Mandiant suggests that as many as 83 million devices could be at risk.

The researchers found that the vulnerability exists for IoT devices that connect to associated mobile apps across the Internet using the ThroughTek "Kalay" network. The protocol is implemented by ThroughTek as a software development kit which third-party developers can use as a means of adding remote access to consumer devices. They also found that because of the way the protocol is implemented by various device-makers, it was impossible to identify the hardware devices that are impacted. The team at Mandiant notes that the problem they found was in the registration mechanism for conversations between devices and the mobile apps that connect to them.

Once the vulnerability was discovered, Mandiant, along with ThroughTek and CISA, notified all of the known third parties who use the Kalay network of the problem. They also provided them with information that would allow them to know if their product was involved. Meanwhile, a team at ThroughTek came up with a patch to fix the problem. Unfortunately, customers who bought and use devices that are impacted by the vulnerability cannot apply the patch themselves—they have to contact the maker of their device to make sure that the patch has been applied.

More information: Mandiant Discloses Critical Vulnerability Affecting Millions of IoT Devices: www.fireeye.com/blog/threat-re … ing-iot-devices.html

Citation: Vulnerability found in IoT devices that use ThroughTek 'Kalay' network (2021, August 18) retrieved 26 April 2024 from https://techxplore.com/news/2021-08-vulnerability-iot-devices-throughtek-kalay.html