Smart home hack: Tuya releases security update

The smart home hardware manufacturer Tuya has released an update designed to close the security holes published on the 35C3.

Perhaps safer in the future: Tuya IoT devices. (Image: Screenshot: heise online)

01/29/2019 6:40 pm

from Jan Mahn and Merlin Schumacher

The manufacturer Tuya, whose smart home devices can mainly be found under other brand names in the trade, wants to close the security gaps that have become known in the in-house IoT platform Smart-Life. According to its own information, the manufacturer published a firmware update for this on Monday. A Tuya spokesman told heise online when the providers who sell Tuya's devices to end

customers under their own brand name and import the new firmware into their devices are up to them.

Tuya is a Chinese manufacturer of smart home and IoT hardware that sells its products as "white label" goods to other companies who then sell the hardware under their own name. Tuya provides the complete platform for this: an app, the cloud backend and the device firmware. The IT startup VTRUST discovered serious security gaps in this firmware and presented them on the 35C3 .

Encryption with additional chips

With an update from January 28th, many of these security problems should be resolved, the manufacturer announced. In future, the new firmware will only transmit data encrypted with TLS. In addition, the firmware should also be able to encrypt data in the flash memory. The ESP8266 microcontroller often used by Tuya cannot protect its flash memory from being read out. In order to secure this data, the providers have to install an external security chip, as Tuya suggests in the statement.

There is another loophole in the update procedure used by Tuya. Over-the-air updates are accepted by the previous firmware without any check, so that the software imports any updates without looking. In the future, a signature check should ensure that only official Tuya updates are imported. According to the announcement, Tuya wants to protect the firmware code with code obfuscation. They also want to update the app in order to secure the keys it contains with a protection system developed in-house.

First corrections in summer?

Nun heißt es: Warten auf die Anbieter. Und das kann möglicherweise dauern: Das Problem der im Klartext übertragenen AES-Schlüssel hat das Unternehmen eigenen Angaben zufolge im August vergangenen Jahres behoben. Bisher ist das Update aber offenbar noch nicht auf den im Handel erhältlichen Geräten angekommen. Die Experimente der c't-Redaktion zeigten, dass die Lücke auch bei neu gekauften Geräten noch bestehen. Auch ist das neue Firmware-Update noch auf keinem der Geräte in der Redaktion eingegangen.

Keine Informationen zur WLAN-Lücke

Tuyas Stellungnahme enthält keine Hinweise auf die schwerwiegendste Schwachstelle: Bei der Einrichtung der Geräte überträgt das Mobiltelefon mit der Tuya-App die WLAN-Zugangsdaten, die der Nutzer zuvor eingegeben hat, über Multicast-Pakete. Entscheidend sind aber nicht die Inhalte der Pakete, sondern die Paketlänge – wer das Prinzip verstanden hat, kann die Zugangsdaten abgreifen, ohne selbst im WLAN angemeldet zu sein.

The scripts used by VTRUST for the hack were revised by in cooperation with c't so that they can be used to install open source firmware such as Tasmota on the devices. The scripts are published on

GitHub , the description is summarized in a c't practical article . To free the Tuya devices from their original software and the cloud, a Linux computer with WiFi, such as a Raspberry Pi, is sufficient. (Mls)

Read comments (18)

To home page

MORE ON THE SUBJECT

35C3 CHAOS COMPUTER CLUB ESP8266 INTERNET DER DINGE SMART HOME

Forum zum Thema: Smart Home

TEILE DIESEN BEITRAG

Kurzlink: https://heise.de/-4292028

DSGVO-konformes Datenlöschen: Löschkonzepte erstellen

heise+ 11 iX Magazin

Ethereum schürfen leicht gemacht: Mining-Guide zum Geldverdienen per Grafikkarte

Liegen die Preise für Kryptowährungen hoch, wirft das private Minen Gewinn ab. Wir zeigen, wie einfach man Ether mit der Grafikkarte errechnet.

heise+ 506

Smarte Heizkörperthermostate im Vergleich: 13 Modelle für die kalte Jahreszeit

Kosten sparen mit smarten Heizkörperthermostaten: Wir vergleichen 13 Modelle, die automatisch die passende Temperatur je nach Tageszeit einstellen.

IPv6: Freigaben mit Namensdienst auf Fritzboxen nutzen

heise+ 5 c't Magazin

Chef-Gehälter 2021: Das verdienen Führungskräfte in verschiedenen IT-Bereichen

nach oben

Aus Gelb wird Weiß: Alte Kunststoffe bleichen

Alle Angebote

IT News

Newsticker

heise Developer

heise Netze

heise Open Source

heise Security

Online-Magazine

heise+

Telepolis

heise Autos

TechStage

tipps+tricks

Services

Stellenmarkt heise Jobs

Weiterbildung

heise Download
Preisvergleich
Whitepaper/Webcasts
DSL-Vergleich
Netzwerk-Tools
Spielen bei Heise
Loseblattwerke
iMonitor
IT-Markt

Heise Medien

heise Shop
Abo
Veranstaltungen
Arbeiten bei Heise
Mediadaten
Presse

Newsletter heise-bot Push messages

data protection Cookies & Tracking imprint Contact Media data 2590064