Disclosure: Security Vulnerability on Tuya IoT Cloud (Resolved)

Sep 15, 2021

Overview

Roborock vacuum cleaners(i.e. devices) connect to either Tuya IoT cloud or Roborock IoT cloud depending on the version of the firmware and Roborock app. For those devices connect to Tuya IoT cloud, the device side library uses an insecure random number generator when negotiating communication channel with the Tuya IoT cloud. This vulnerability affects a portion of Roborock product models globally. Those devices connected to Roborock IoT cloud are not affected by this vulnerability.

Threat

This issue undermines the security of the user data transmitted on the channel between the device and Tuya IoT cloud, including device info, cleaning data, maps, robot settings and customization options.

Affected Models

This issue affects the following products

- Roborock S6
- Roborock S5 Max
- Roborock S6 Pure
- Roborock S6 MaxV
- Roborock S4

How can users check which IoT cloud they are connected to:

- Users connected to Roborock IoT cloud are not affected by this vulnerability, and so they might not receive the update information.
- For users connected to Roborock IoT cloud,the DID is a string prefixed with "rr_".

Note:DID is a unique device ID assigned by the IoT cloud during the process of network p airing which may change subject to the device, the user and the IoT cloud.

- How to check the DID: Tap the 3 dots at the top right corner of the main page on the Rob orock app, tap "Customer Support" and then "Serial Number" or "Product Info".
- For users connected to Tuya IoT cloud,the DID is a string prefixed with "ty_".

Solution

We have updated the Tuya library to use a more secure random number generator when negotiating communication channel with the IoT cloud.

The solution has been released in full to our customers in the form of a new OTA firmware version.

Fixed versions:

- Roborock S6, via firmware update 01.28.10
- Roborock S5 Max, via firmware update 02.15.16
- Roborock S6 Pure, via firmware update 02.13.26
- Roborock S6 MaxV, via firmware update 01.60.52
- Roborock S4, via firmware update 01.05.68

How can Roborock customers obtain the fix:

1. Roborock customers with the above models should check within their Roborock app for the latest version of the firmware.
2. Roborock customers should update the firmware to the latest version for their respective models, as laid out above.

Note: Customers whose Roborock devices are connected to the Roborock IoT cloud might not receive the above-stated firmware version as they are not affected by this vulnerability.

Credit

Credit goes to JPCERT Coordination Center (https://jvn.jp,https://jvn.jp/en/) who first highlighted this vulnerability.

Contact Information

For additional support, please contact us at security@roborock.com.