CVE-2019-9659: Chuango burglar alarm replay vulnerability in RF remote control/sensor protocol

Overview

Security Researcher Riccardo ten Cate discovered a vulnerability in Chuango's burglar alarm product line. Due to the use of fixed code in the RF remote control protocol an attacker is able to arm, disarm or trigger the alarm remotely. This vulnerability has been assigned a CVSSv3 base score of 9.1 (critical) with vector string CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

Affected Products

Chuango reports that all products employing 433MHz RF technology manufactured to date (Feb 25, 2019) are vulnerable. The affected models include but are not limited to:

- Chuango Wifi Alarm System
- Chuango Wifi/Cellular Smart Home System H4 Plus
- Chuango Wifi Alarm System AWV Plus
- Chuango G5W 3G
- Chuango GSM/SMS/RFID Touch Alarm System G5 Plus
- Chuango GSM/SMS Alarm System G3
- Chuango G5W
- Chuango Dual-Network Alarm System B11
- Chuango PSTN Alarm System A8
- Chuango PSTN/LCD/RFID Touch Alarm System A11
- Chuango CG-105S On-Site Alarm System

As OEM Chuango manufactures similar devices for other manufacturers. The following brands/models are known to be affected:

- Eminent EM8617 OV2 Wifi Alarm System

Impact

An attacker could remotely disable the burglar alarm through the Radio Frequency remote function, defeating the primary function of the product.

Background

Established in Fuzhou, China in 2001, Chuango Security Technology Corporation specializes in wireless smart home technology, ranging from DIY security and home automation to energy and health management systems.

Timeline

December 6, 2018	Vulnerability discovery
December 7, 2018	Attempt to contact Chuango (by e-mail and phone)
December 18, 2018	Initial contact with General Manager Chuango Europe
January 9, 2018	Shared vulnerability details with product security contact Chuango

January 15, 2019	Shared PoC with product security contact Chuango
January 15, 2019	Shared vulnerability details with Eminent
January 28, 2019	Sent reminder and request for status update
January 29, 2019	Acknowledgement by Eminent
February 11, 2019	Confirmation of vulnerability on all devices using 433MHz RF technology. No after sales fix will be provided.
February 17, 2019	Sent reminder to Chuango and another request for fix timeline.
March 11, 2019	CVE ID assigned
March 11, 2019	Details shared with consumers' associations, public disclosure

Contact information

Riccardo ten Cate - riccardotencate@gmail.com
Mattijs van Ommeren – mattijs.vanommeren@nixu.com