# Trustworks KG Security Advisory

| | |
|---|---|
| Title: | Predictable AES-128 Key, wireless cloning |
| Product: | Hoermann BiSecur |
| Vulnerable Version: | BiSecure radio transmitters with manufacturing dates before 2018 |
| Fixed Version: | BiSecur radio transmitters manufactured 2018 or later |
| CVE number: | CVE-2017-17910 |
| CVSS2 Score: | 9.7 |
| CVSS2 Vector: | (AV:N/AC:L/Au:N/C:C/I:C/A:P) |
| Impact: | Critical |
| Vendor Homepage: | http://www.hoermann.com |
| Found: | 2017-10-04 |
| By: | Markus Muellner, Markus Kammerstetter, Christian Kudera and Daniel Burian<br>Trustworks KG<br>https://www.trustworks.at |

## Vendor description:

"In the market for construction components, more and more gates, doors, frames and operators carry the Hoermann name, making the Hoermann Group Europe's largest provider of such products. This leadership has been attained through decades of continuous growth as a result of innovation, ensured quality and proximity to the customer."Predictable AES-128 Key, wireless cloning

Source: http://www.hoermann.com/

## Product description:

“The bi-directional radio system BiSecur is based on future-oriented technology for the convenient and secure operation of garage and entrance gate operators, door operators, lights and more. This extremely secure BiSecur encryption protocol, developed by Hoermann, with a stable, interference-free range makes sure that no-one can copy your radio signal.”

Source: http://www.hoermann.lv/fileadmin/_country/hoermann.uk/kataloge/86971-BiS-SmartHome-EN.pdf

## Vulnerability description:

The Hoermann BiSecur radio system uses a proprietary encryption scheme, with the AES-128 algorithm at its core, to secure the radio communication between transmitter and receiver. During an initial key generation process or a device reset, the transmitter utilizes a key generation algorithm based on the proprietary Hoermann encryption scheme to generate a new encryption key. The key is used to protect any subsequent radio communication between transmitter and receiver.

The key generation algorithm uses a static initial 80-bit random value, a static 128-bit data vector (both are common to all observed Hoermann BiSecur transmitters) and the individual 32-bit serial number (transmitted in the clear during all transmissions).

The vulnerability can be exploited by recording a single radio transmission. An attacker can thus intercept an arbitrary radio frame exchanged between a BiSecur transmitter and a receiver to obtain the encrypted packet and the 32-bit serial number. The interception of the one-time pairing process is specifically not required. Due to the initial static random value and the static data vector (common to Hoermann BiSecur transmitters), the attacker can easily derive the utilized encryption key and decrypt the intercepted packet. The key can be verified by decrypting the intercepted packet and checking for known plaintext.

Subsequently, an attacker can create arbitrary radio frames with the correct encryption key to control BiSecur garage and entrance gate operators and possibly other BiSecur systems as well.
To conduct the attack, a low cost Software Defined Radio (SDR) is sufficient.

Vulnerability impact:
--------------------------

- Over the air cloning of transmitters (“copying of radio signal”)
- Unauthorized control and access to garage and entrance gates
- Likely impact on other BiSecure devices including SmartHome devices (untested)
- Denial of Service: By advancing the rolling counter value to a value outside the accepted window (between the genuine transmitter and the receiver), the genuine transmitter can no longer control the receiver as its transmitted counter value will be lower than the counter values that are accepted by the receiver.

Proof of concept:
-----------------

Due to the high number of affected BiSecur systems and users, we do not provide a proof-of-concept exploit.

Vulnerable / tested devices:
----------------------------

The following devices have been tested and are known to be vulnerable:

Hoermann Hand Transmitter HS5-868-BS
Hoermann Hand Transmitter HSE1-868-BS
Hoermann Hand Transmitter HSE2-868-BS

Vendor contact timeline:
------------------------

2017-10-04: Involving the Austrian national CERT team as coordinator, we reported the security vulnerability including a detailed advisory and a suggested security fix so that the manufacturer can fix the issue.

2017-10-31: Confirmation from CERT that the manufacturer received and understood the security problem.

2017-11: Various e-mails and phone calls with manufacturer.

2017-11-30: Meeting with manufacturer - we presented the vulnerability and the suggested security fix.

2017-12: Confirmation from manufacturer - security fix has been implemented and is in testing phase.

2017-12-28: Public presentation of the vulnerability at the 34C3 conference.

Solution:
---------

According to the manufacturer, a security fix has been implemented.
Customers should thus contact the manufacturer.

Workaround:
-----------

Not available.

Advisory URL:
-------------

https://www.trustworks.at/publications

-----------------------------------------------------------------------------------
Trustworks KG

Rienoesslgasse 14/17
1040 Vienna, Austria

Mail: office -at- trustworks.at
PGP Key-Id: 989a04a6
PGP Fingerprint: 9BCB 782D 6E3A 5FAB C11C 3754 FD5F B9E1 989A 04A6