OpenSource Security Ralf Spenneberg

Am Bahnhof 3-5

48565 Steinfurt

info@os-s.net

English text below

OS-S Security Advisory 2016-01

Datum: 1. Januar 2016

Letzte Aktualisierung: 1. Januar 2016

Autoren: Hendrik Schwartke, Ralf Spenneberg

CVE: Noch nicht zugeteilt

CVSS: 6.2 (AV:L/AC:L/Au:S/C:C/I:C/A:N)

Titel: Fehlerhafte Integritätssicherung bei Uhlmann & Zacher Clex prime Schließanlage mit 125 kHz EM4450 Transpondern

Schweregrad: Kritisch. Die Schließberechtigungen können beliebig manipuliert und erweitert werden.

Komplexität des Angriffs: Einfach

Schwachstelle: Fehlerhafte Integritätssicherung

Produkt: U&Z Clex prime Schließanlage mit 125 kHz EM4450 Transponder

Nicht-Technisch Beschreibung

Die Clex prime Schließanlage weist bei Nutzung des 125kHz EM4450 Transponders Schwachstellen auf, die eine nicht-autorisierte Erzeugung von Schlüsseln und die Manipulation von Schließberechtigungen durch einen Angreifer erlauben. Für einen erfolgreichen Angriff muss der Angreifer folgende Voraussetzungen haben:

- Kurzzeitiger Besitz eines für die Schließanlage programmierten Schlüssels (beispielsweise auch verlorener Schlüssel)
- Besitz von Hardware und Software zum Abhören der 125kHz - Kommunikation zwischen Schloss und Schlüssel
- Kenntnis über den Algorithmus zum Bilden der Prüfsumme
- Kurzzeitiger, unbeobachteter Zugang zu einem Schloss des Schließsystems, um mit der Abhörhardware einen Verbindungsversuch mitzuprotokollieren

Schwachstellen in den eingesetzten Verfahren zur Integritätssicherung und Verschlüsselung können von einem Angreifer zur gezielten Manipulation und zur Kopie der Schlüssel genutzt werden. Diese Schwachstellen wurden durch das Unternehmen „OpenSource Security Ralf Spenneberg“ erkannt und an den Hersteller Uhlmann & Zacher GmbH gemeldet, der diese Schwachstellen nachvollzogen hat und ein Update zur Verfügung stellt. Das Update wurde im Auftrag von der Uhlmann & Zacher GmbH von „OpenSource Security Ralf Spenneberg“ geprüft. Die Behebung der Schwachstelle erfordert ein Firmware-Update der eingesetzten Schließzylinder, ein Update der Keyvi3 Software, einen Austausch des Servicekeys und ein Update der Daten auf den Schlüsseln in Benutzung.

Clex prime Schließanlagen mit Mifare DESFire und Legic advant Technologie sind von der Schwachstelle nicht betroffen.

Technischer Hintergrund

Die Clex prime Schließanlage kann mit unterschiedlichsten Transpondertechnologien eingesetzt werden. Die 125kHz Variante erlaubt bei Einsatz des EM4450 Transponders einem Angreifer beliebige Schlüssel zu erzeugen. Um die Vertraulichkeit und Integrität der Schließberechtigungen auf dem Transponder zu schützen werden drei verschiedene Verfahren eingesetzt:

1. Der Transponder bietet einen Kennwortschutz der gespeicherten Daten. Dieses Kennwort kann jedoch bei kurzzeitigem Zugang zu einem beliebigen Schließzylinder der Anlage durch geeignete Hardware ausgelesen werden.

2. Die Daten auf dem Transponder verfügen über eine Prüfsumme, die eine Manipulation oder Kopie der Daten erkennt. Bei Kenntnis des eingesetzten Algorithmus kann ein Angreifer diese Prüfsumme korrekt berechnen. Eine Manipulation oder Kopie der Daten kann durch die Anlage außer bei der Analyse von Ereignisprotokollen nicht mehr erkannt werden.

3. Alternativ zur Prüfsumme können die Daten auf dem Transponder verschlüsselt werden. Da in diesem Fall keine Prüfsumme genutzt wird, kann ein Angreifer durch gezielte Manipulation des Cipher-Block-Chaining Modes beliebige Schließberechtigungen setzen oder löschen.

Herstellerkontakt

Wir kontaktierten den Hersteller erstmalig im Oktober 2014. Die letzten Schwachstellen wurden am 15. April 2015 an den Hersteller gemeldet.

OpenSource Security Ralf Spenneberg

Am Bahnhof 3-5

48565 Steinfurt

info@os-s.net

OS-S Security Advisory 2016-01

Date: January 1st, 2016

Updated: January 1st, 2016

Authors: Hendrik Schwartke, Ralf Spenneberg

CVE: Not yet assigned

CVSS: 6.2 (AV:L/AC:L/Au:S/C:C/I:C/A:N)

Title: Insufficient integrity checks in Uhlmann & Zacher Clex prime locking systems using 125 kHz EM4450 transponders

Severity: Critical. The locking permissions may be arbitrarily manipulated and extended.

Ease of Exploitation: Trivial

Vulnerability: Insufficient integrity protection

Product: U&Z Clex prime locking system using 125 kHz EM4450 transponder

Non-Technical Description

The Clex prime locking system has several vulnerabilities which allow an attacker to generate keys and to arbitrarily manipulate the locking permissions without authorization. For the successful attack the following requirements need to be met:

- Brief possession of a (former) valid key of locking system. A lost and revoked key will work as well.
- Access to hardware and software to sniff the 125kHz communication between the lock and the key.
- Knowledge of the algorithm to calculation the checksum
- Brief unobserved access to a lock of the locking system to sniff and log a communication attempt.

Vulnerabilities in the algorithms used for integrity protection and encryption may be used

by the attacker for targeted modification and copying of a key. These vulnerabilites have been found by OpenSource Security Ralf Spenneberg and reported to the vendor Uhlmann & Zacher GmbH. The vendor as reproduced the vulnerabilities and provided an updated version. Uhlmann & Zacher GmbH tasked OpenSource Security Ralf Spenneberg to check the update.

The removal of the vulnerability requires a firmware update of the used locks, the update of the Keyvi3 software, the replacement of the servicekeys and an update of all keys in use.

Clex prime locking systems using Mifare DESFire and Legic advant technology are not affected by this vulnerability.

Technical Background

The Clex prime locking system may be used with different transponder technologies. When using the 125 kHz variant with the EM4450 transponder an attacker may create arbitrary keys for the locking system.

To protect the confidentiality and integrity of the locking permissions stored on the transponder three different methods are used:

1. The transponder provides access protection using a password. The password can be retrieved over the air by an attacker having brief access to a lock of the locking system using appropiate hardware.

2. The data on the transponder is protected by a checksum. Manipulation of copying of the locking permissions to a different transponder is detected. With the knowledge of the underlying checksum algorithm the attacker may calculate a valid checksum. The manipulated or copied data is then not detected by the locking system anymore. Only the analysis of the protocols may allow the detection.

3. Alternative to the checksum the data on the transponder may be encrypted. Since no checksum is used in this mode targeted manipulation of the Cipher-Block-Chaining may be used to set or remove specific locking permissions.

Vendor Contact

We contacted the vendor the first time in October 2014. The last vulnerabilities were reported to the vendor on April 15th 2015.