OpenSource Security Ralf Spenneberg

Am Bahnhof 3-5

48565 Steinfurt

info@os-s.net

English text below

OS-S Security Advisory 2016-03

Datum: 1. Januar 2016

Letzte Aktualisierung: 1. Januar 2016

Autoren: Oguzhan Cicek, 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 Winkhaus Bluesmart Schließanlagen mit Hitag S Transponder

Schweregrad: Kritisch. Schließberechtigungen und Zeitfenster können nach Modifikation durch die Anlage im Original wiederhergestellt werden.

Komplexität des Angriffs: Einfach

Schwachstelle: Fehlerhafte Integritätssicherung

Produkt: Winkhaus Bluesmart mit Hitag S und Bluecontrol Start Virtuell 5.2.0

Zusammenfassung

Die Winkhaus Bluesmart Schließanlage speichert die Schließberechtigungen und die Zeitfenster, in denen die Schließberechtigungen ausgeübt werden dürfen auf einem Hitag S Transponder in der Spitze des verwendeten Plastikschlüssels. Kann ein Angreifer entsprechend unserem Advisory 2016-2 auf die Daten eines Schlüssels zugreifen und diesen auslesen, kann er auch die dort gespeicherten Schließberechtigungen und Zeitfenster auslesen. Diese sind durch Verschlüsselung gegen Modifikation geschützt. Werden diese Berechtigungen oder Zeitfenster später durch die Schließanlage eingeschränkt, kann der Angreifer die originalen Berechtigungen wiederherstellen. Die Schlösser erkennen diese Manipulation nicht.

Szenario

Häufig werden bei der Neuinstallation einer RFID-basierten Schließanlage nicht sofort alle

erforderlichen Schließberechtigungen ermittelt und den Anwendern entsprechend zugeteilt. In vielen Umgebungen werden bei Neuinstallationen, um den Organisationsaufwand gering zu halten, häufig allen Anwendern sämtliche Schließberechtigungen für einen unendlichen Zeitraum gewährt. Die Schließberechtigungen und die erlaubten Zeiträume werden dann im Nachgang eingeschränkt. Speziell bei dem Winkhaus Bluesmart ist diese Vorgehensweise wahrscheinlich, da das System ein Auladegerät verwendet, mit dessen Hilfe die Anwender jeden Tag erneut ihre Berechtigungen und Zeitfenster auf den Transponder übertragen bekommen können.

Ein Angreifer kann nach der so erfolgten Einschränkung der Berechtigungen diese wiederherstellen, ohne das die Schlösser die Manipulation erkennen können.

Technischer Hintergrund

Das Memory-Layout der Winkhaus Schlüssel hat folgenden Aufbau:

	0	1	2	3
0	UID	PH0 Con2, 1, 0	KH 1,0 PL 1,0	KL 3,2,1,0
1	00 00 00 00	00 00 00 00	XX 03 01 07	02 18 00 XX
2	Zeitstempel			
3	00 00 00 00	00 00 00 00	00 00 00 00	00 XX XX XX
4	Schloss -> Aufladestation			
...				
8				
9	Aufladestation -> Schloss			
...				
14				
15	Schließberechtigungen			

Legende: Lese-Schutz AES-Verschlüsselt Winkhaus ID

Die rot dargestellten Informationen sind vor dem Auslesen geschützt. Die grau schraffierten Informationen werden durch die Anlage AES-verschlüsselt. Hierbei werden die Zeitfenster und die Schließberechtigungen in unterschiedlichen Bereichen gespeichert. Diese können bei Kenntnis einer gültigen Authentifizierungschallenge in einem Replay-Angriff oder bei Kenntnis des Schlüssel gelesen und geschrieben werden. Ein Kopieren der Daten auf einen anderen Schlüssel wird durch das System erkannt.

Herstellerkontakt

Wir kontaktierten Winkhaus am 13. Juli 2015 telefonisch. Am 16. Juli 2015 erläuterten wir dem Hersteller unsere Erkenntnisse in einem persönlichen Gespräch.

OpenSource Security Ralf Spenneberg

Am Bahnhof 3-5

48565 Steinfurt

info@os-s.net

OS-S Security Advisory 2016-03

Date: January 1st, 2016

Updated: January 1st, 2016

Authors: Oguzhan Cicek, 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 Protection in Winkhaus Bluesmart locking systems using Hitag S

Severity: Critical. The locking permissions may be restored by the attacker after modification by the system

Ease of Exploitation: Trivial

Vulnerability: Insufficient integrity protection

Product: Winkhaus Bluesmart using Hitag S and Bluecontrol Virtuell 5.2.0

Abstract

The Winkhaus Bluesmart locking system stores the locking permissions and the time windows, when the permissions may be executed, on a Hitag S transponder located oin the tip of the plastic key. If an attacker is able to extract the data stored on the transponder according to our advisory 2016-2 he also has access to the locking permissions and time windows. Although the information is protected against manipulation via encryption, if the permissions or the time windows are modified by the system later the attacker is still able to restore the orginal permissions and time windows. The locks will not detect this manipulation.

Scenario

Often when deploying a new RFID based locking system not all required locking permissions are known. To ease the launch very often all users get initially global almost unlimited access. The actually required permissions are analyzed and then enforced in a

second step. This is especially true in case of the Winkhaus Bluesmart system. Here the users may be required to retrieve new permissions and time windows in a daily routine using a special reader.

The attacker may restore his original permissions and time windows if such a restriction took place. The locks do not detect the modification of these permissions.

Technical Background

The memory layout of the transponder used by the Winkhaus Bluesmart is shown below:

	0	1	2	3
0	UID	PH0 Con2, 1, 0	KH 1,0 PL 1,0	KL 3,2,1,0
1	00 00 00 00	00 00 00 00	XX 03 01 07	02 18 00 XX
2	Zeitstempel			
3	00 00 00 00	00 00 00 00	00 00 00 00	00 XX XX XX
4	Schloss -> Aufladestation			
...				
8				
9	Aufladestation -> Schloss			
...				
14				
15	Schließberechtigungen			

Legende: Lese-Schutz AES-Verschlüsselt Winkhaus ID

The red information is read-protected. The grey areas are encrypted using AES. The time windows and the locking permissions are stored in different areas. They may be read and written using a replay attack or if the actual Hitag-S key has been broken. Copying the data to a different key is detected by the system.

Vendor contact

We reached out to Winkhaus on Juli 13th, 2015 via phone. On Juli 16th, 2015 we elaborated our findings in a personal meeting.