IOActive Security Advisory

Title	Replay Attack in SimpliSafe Alarm System
Severity	High
Discovered by	Dr. Andrew Zonenberg
Advisory Date	17 February 2016

Affected Products

1. SimpliSafe home burglar/fire alarm systems

Overview

SimpliSafe manufactures a line of wireless alarm systems and sensors targeted at home users, and provides a monitoring service to contact emergency services if an alarm is triggered. The service is marketed as an easy-to-install, more secure alternative to other alarm systems which require running wires throughout the house.

However, the radio interface is not encrypted and does not use “rolling codes,” nonces, two-way handshakes, or other techniques to prevent transmissions from being recorded and reused. An attacker who is able to intercept the radio signals between the keypad and base station can record and re-play the signal in order to turn off the alarm at a time of his choice in the future.

Technical Details

The keypad and sensors communicate with the base station in cleartext via a 433 MHz digital radio. An attacker who is within radio range of the alarm system can record these packets, examine the header to determine the type of message, and then play it back on demand to disable the alarm, trigger false alarms, and otherwise take full control of the system. The transmitter on the keypad circuit board and receiver on the base station can be combined with an off-the-shelf microcontroller board to implement this attack at minimal cost (less than $250 in parts and a few hundred lines of code).

This attack requires physical proximity to the target system and cannot be performed over the Internet. However, since a criminal must obviously enter the protected property in order to burglarize it, physical proximity does not significantly increase the difficulty of the attack.

Fixes

SimpliSafe should release new firmware which adds cryptographic protections to prevent packets from being recorded and replayed. Unfortunately it appears that the deployed systems use one-time-programmable microcontrollers, which means that field updating of

existing systems is not possible. All existing keypads and base stations will need to be replaced to fix the vulnerability.

Mitigation

By changing PINs often the useful lifetime of a captured PIN can be reduced, but this does not stop an attacker from intercepting the new PIN after the change.

Timeline

- August 26, 2015 – IOActive researcher Dr. Andrew Zonenberg discovers vulnerability.
- September 3, 2015 – First attempt to contact vendor.
- September 18, 2015 – Second attempt to contact vendor.
- October 5, 2015 – Third attempt to contact vendor.
- October 15, 2015 – Notified ICS-CERT of critical vulnerability and failed attempts to contact vendor.
- October 27, 2015 – ICS-CERT confirms that report with vulnerability ID ICS-VU-045410 was being forwarded to US-CERT.
- February 17, 2016 – After receiving no response from multiple attempts to contact the vendor over five months, IOActive advisory is published.

