tenable

SimpliSafe SS3 PIN Add Using Rogue Keypad

Low

← View More Research Advisories

Synopsis

We have discovered a vulnerability in SimpliSafe SS3 which is an incomplete fix to TRA-2020-03.

An attacker, with **physical access**, can add PINs without prior knowledge of the PIN. **This allows the attacker to disarm the system.**

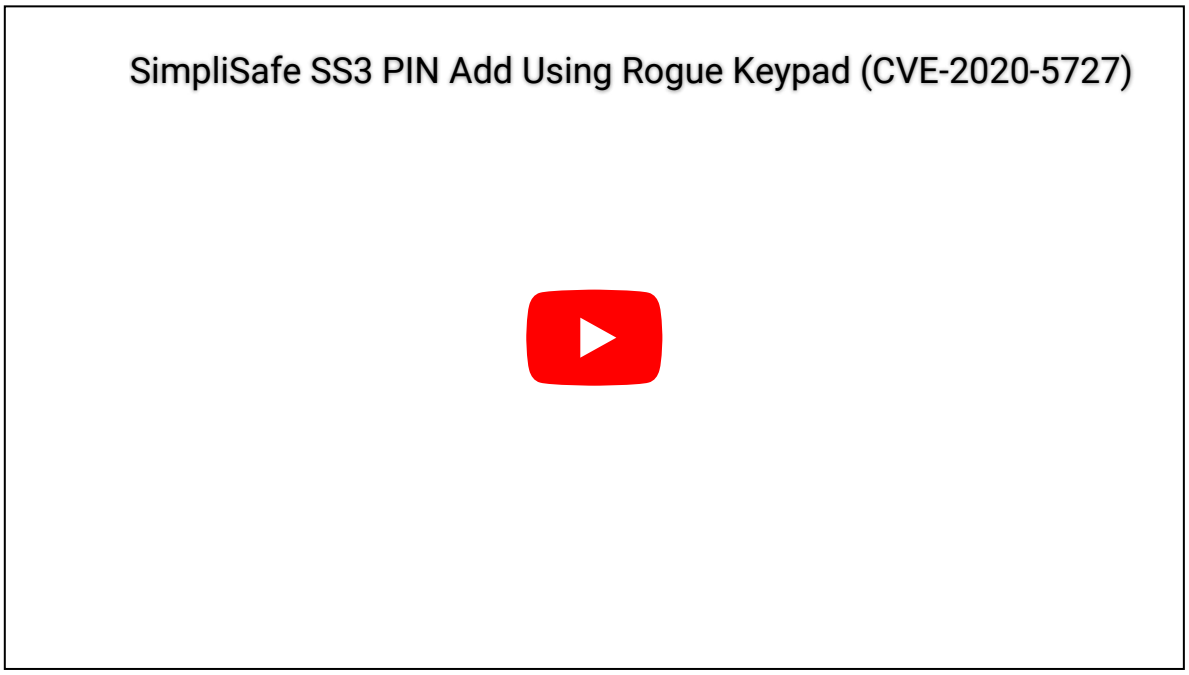
There is a button on the bottom of the base station (next to the batteries) that, after being pressed, will allow new devices to be paired. Specifically, **a rogue keypad (which is already paired to another base station) can be added** to facilitate the attack. While paired to both base stations, the attacker can add PINs to the victim base station. This can be accomplished with a victim system armed as "away" or "home".

Also, please note that we could not complete the full attack in under 30 seconds (default entry delay before the alarm triggers). This limits attackers to an **insider threat**. A more feasible scenario is that an attacker could pair the rogue keypad while in the house, and disable the alarm at a later date (e.g. when burglarizing).

Proof of Concept

Note: In our testing, the victim and attacker systems had different versions. The victim was fully patched, while the attacker is out of date.

```
Victim: Keypad 1.4.20, base station 1.4.62
Attacker: Keypad 1.2.16, base station 1.3.2
```



Follow the steps below to disable an armed base station.

Assumptions:

1. There is a "victim" base station ("BS1") with a keypad ("KP1") already paired.
2. There is an "attacker" base station ("BS2") with a keypad ("KP2") already paired.

Instructions:

1. Arm BS1 in "home" mode.
2. Power down BS2.
3. Power down KP2.
4. Remove the bottom cover of BS1 to reveal the battery compartment. Press the small white circular button to enable pairing of new devices.
5. Power on KP2. After the power on sequence completes, it should pair to BS1.
6. After KP2 pairs, turn on BS2.
7. Reboot KP2.
8. After KP2 powers on, the display should say "off" (indicating it's talking to BS2).
9. Press "menu", and enter the PIN for BS2.
10. Select "PINs"
11. Modify the Master PIN to a new value or add/modify a user PIN.
12. Back out of the menu.

Solution

Upgrade to system firmware 1.6

Additional References

https://simplisafe.com/forum/customer-support-forum/installing-and-using-simplisafe/firmware1_6-april2020
https://www.tenable.com/security/research/tra-2020-03

Disclosure Timeline

01/16/2020 - Vulnerability discovered and disclosed. 90-day date is 04/15/2020.
01/17/2020 - SimpliSafe indicates we encrypted the wrong document.
01/17/2020 - Yes, we did. Tenable resends disclosure. Pushes 90-day date by 1 day. 04/16.
01/23/2020 - Tenable asks if report was received.
01/23/2020 - Yes, the report was received.
02/04/2020 - SimpliSafe was able to reproduce.
02/06/2020 - Tenable acknowledges. Asks for clarification.
02/07/2020 - SimpliSafe provides clarification.
02/07/2020 - Tenable thanks SimpliSafe.
03/19/2020 - Tenable asks for an update.
03/31/2020 - The fix will be in the next firmware release, but a specific date is not known yet.
04/13/2020 - SimpliSafe says they will tentatively release on the 20th. Asks if we will hold off on disclosure.
04/13/2020 - Sure, no problem.
04/21/2020 - SimpliSafe says there are some issues with the beta, and they'll need to push the release. Asks if we can hold disclosure.
04/21/2020 - Sure, we can. When will it be released?
04/21/2020 - Simplisafe says hopefully by the end of the week. Thanks us for coordinating.
04/22/2020 - Tenable acknowledges. Thanks SimpliSafe for open communication.
04/27/2020 - Tenable asks for an update.
04/27/2020 - SimpliSafe says a staggered rollout is expected to start today and over the next 2 weeks. How does Tenable handle such deployment models?
04/27/2020 - Tenable asks for details about the deployment model.
04/27/2020 - SimpliSafe provides more info.
04/27/2020 - Tenable thanks SimpliSafe. We will release an advisory if patches are distributed to any customers. We would also appreciate a heads up when customers receive the patch, so we can coordinate an advisory.
05/01/2020 - Tenable notices that SimpliSafe notified their customers on April 29 about system firmware update 1.6. It is being rolled out to all customers.

Risk Information

CVE ID: CVE-2020-5727
Tenable Advisory ID: TRA-2020-29
Credit: Chris Lyne

CVSSv2 Base / Temporal Score: 1.9 / 1.5
CVSSv2 Vector: (AV:L/AC:M/Au:N/C:N/I:P/A:N)
Affected Products: SimpliSafe (SS3) firmware prior to 1.6
Risk Factor: Low

Advisory Timeline

05/01/2020 - Advisory published
05/04/2020 - Typo fixed in disclosure timeline

Application Security
Building Management Systems
Cloud Security Posture Management
Compliance
Exposure Management
Finance
Healthcare
IT/OT
Ransomware
State / Local / Education
US Federal
Vulnerability Management
Zero Trust
→ View all Solutions

CUSTOMER RESOURCES

Resource Library
Community & Support
Customer Education
Tenable Research
Documentation
Trust and Assurance
Nessus Resource Center
Cyber Exposure Fundamentals
System Status

CONNECTIONS

Blog
Contact Us
Careers
Investors
Events
Media