SimpliSafe Advisory No. 20180321

Revision 1.8
Last Updated 2018 August 21 15h00 UTC (GMT)
For LIMITED Release 2018 August 24 00h00 UTC (GMT)

Wireless capture-replay authentication bypass, wireless radio frequency interference service interruption, and physical base station disconnect service interruption in the SimpliSafe® Original Home Security System [CVE-2018-11399; CVE-2018-11400; CVE-2018-11401; CVE-2018-11402]. This advisory does not apply to the All New SimpliSafe Home Security System, which was first sold in January 2018, or the SimpliCam® security camera, as these products are not affected by the vulnerabilities listed in this advisory. This has been validated by external security experts.

Overview

In March 2018, known vulnerabilities in SimpliSafe Original Sensors, Keypad, and Base Station, which were first reported in February 2016 by Dr. Andrew Zonenberg (IOActive), and then by Michael Ossmann (Great Scott Gadgets), were re-submitted to SimpliSafe by Adam Callis.[1] This advisory integrates Mr. Callis' findings with respect to the SimpliSafe Original Home Security System with prior research, describes the validation of those findings performed by a specialist hardware and wireless/RF security research team, enumerates affected products, and describes mitigation recommendations for customers of the SimpliSafe Original Home Security System.

Importantly, this advisory updates SimpliSafe's suggested mitigations from its initial response in February 2016.[2] While Mr. Callis reported no new vulnerabilities and did not demonstrate attacks of significantly lesser complexity or greater efficacy, SimpliSafe acknowledges that as time and technology progress, attacks against exposures such as those in the SimpliSafe Original system may tend to become more practical.[3]

Though this is an increasingly accessible area of security research, SimpliSafe is not aware of customers compromised using the methods described in this advisory. Additionally, even though these vulnerabilities are present in other similar home security products, Simplisafe is unaware of any compromise against similar home security products using these methods.

SimpliSafe discontinued manufacturing the SimpliSafe Original Home Security System in 2017 and removed the product from prominent display on its website. More recently, SimpliSafe made the decision to offer a **deep upgrade discount to existing customers of the SimpliSafe Original Home Security System**. Details regarding subsidized upgrade paths and other

[1] https://www.simpleorsecure.net/simplisafe-security-advisory/
[2] SimpliSafe blog, 'Our Commitment to Your Safety,' 19 February 2016.
[3] In the course of his research, Mr Callis contributed support for the SimpliSafe™ Original devices tested to a popular open-source repository of over 100 various protocol decoder modules for use with low-cost software-defined radio (SDR) dongles. https://github.com/merbanan/rtl_433

SimpliSafe Advisory No. 20180321
Revision 1.8
Last Updated 2018 August 21 15h00 UTC (GMT)
For LIMITED Release 2018 August 24 00h00 UTC (GMT)

accommodations for owners of SimpliSafe Original Home Security Systems were provided to affected customers.

SimpliSafe takes a proactive approach to security and devotes extensive engineering and testing resources, using both internal and external expertise, to secure its products using industry best practices. The All New SimpliSafe home security system and SimpliCam security camera are not affected by the vulnerabilities listed in this advisory; this has been validated by external security experts.

Description

Unencrypted radio frequency (RF) transmissions in SimpliSafe Original Home Security Systems are susceptible to traffic capture and replay by a physically proximate (15-30m), but unauthenticated attacker using a software-defined radio (SDR) dongle loaded with publicly-available code. The equipment required to exploit this vulnerability are relatively low-cost and are made generally available to the public for sale. This attack was validated by SimpliSafe through a third-party security firm. *(Scenario 1)*

Commands entered on the keypad, including ARM, DISARM, TEST MODE, and the PIN code, may be captured by a proximate attacker, as they are transmitted unencrypted to the Base Station of the SimpliSafe Original Home Security System. ARM, DISARM, and PANIC commands transmitted from the Keychain Remote to the Base Station of the SimpliSafe Original home security system, and status information (ACTIVE/OPEN, INACTIVE/CLOSED) transmitted from Entry, Motion, and Water Detector Sensors to the Base Station of the SimpliSafe Original Home Security System, may likewise be captured using similar procedures. Keypad and Sensor serial numbers of the SimpliSafe Original Home Security System are also obtainable via this method. This attack was validated by SimpliSafe through a third-party security firm. *(Scenario 1)*

Transmissions between the Keypad, Keychain Remote, Sensors, and Base Station of the SimpliSafe Original Home Security System are susceptible to interference by radio transmissions over the same frequencies. While an attacker could potentially leverage this attack to make the SimpliSafe Original Home Security System susceptible to being disabled, it is theoretically possible (though unlikely) that legitimate transmissions from amateur radio operators could also have a disruptive effect if sufficiently proximate to a system. However, the SimpliSafe Original Home Security System does attempt to mitigate interference by resending messages. Additionally, the Base Station of the SimpliSafe Original Home Security System can provide notification when RF ‘noise’ impacts its ability to ‘hear’ transmissions from Sensors or other components of the SimpliSafe Original Home Security System, though this is not enabled by default. This attack was validated by SimpliSafe through a third-party security firm. *(Scenario 2)*

It is additionally possible to physically disarm the SimpliSafe Original Home Security System by removing the battery and disconnecting external power if the attacker has access to the Base Station during the “entry delay” period (default is 30 seconds, but timing is configurable). The Base Station of the SimpliSafe Original Home Security System does not alert the system owner to physical tampering. *(Scenario 3)*

Affected products

SimpliSafe Original Home Security System Product Name	FCC ID
SimpliSafe Original Home Security System Base Station	U9K-BS1000; U9K-BS2000
SimpliSafe Original Home Security System Wireless Keypad	U9K-KP1000
SimpliSafe Original Home Security System Keychain Remote	U9K-KR1; U9KR2
SimpliSafe Original Home Security System Carbon Monoxide Sensor	U9K-CO1000
SimpliSafe Original Home Security System Entry Sensor	U9K-ES1000
SimpliSafe Original Home Security System Wireless Freeze Sensor	U9K-FS1000
SimpliSafe Original Home Security System Glassbreak Sensor	U9K-GB1000
SimpliSafe Original Home Security System Motion Sensor	U9K-MS1000
SimpliSafe Original Home Security System Panic Button	U9K-PB1000
SimpliSafe Original Home Security System Smoke Detector	U9K-SD1000
SimpliSafe Original Home Security System Wireless Water Sensor	U9K-WT1000

Impact

Scenario 1

Vulnerability : cve.mitre.org CVE-2018-11399; CVE-2018-11402 [4]	
Provenance : https://ioactive.com/pdfs/IOActive_Advisory_SimpliSafe-Replay.pdf; https://greatscottgadgets.com/2016/02-19-low-cost-simplisafe-attacks/	
Scenario : 1	The first scenario
Product :	SimpliSafe Original Home Security System

[4] SimpliSafe have assessed that both CVE-2018-11399 and CVE-2018-11402 refer to the same exposure; this assessment has been validated by a third-party security firm. For the purposes of mitigation, these two CVEs may be considered as one.

cpe.nist.gov cpe:2.3:h:simplisafe:base_station:U9K-BS1000 cpe:2.3:h:simplisafe:base_station:U9K-BS2000 cpe:2.3:h:simplisafe:keypad:U9K-KP1000 cpe:2.3:h:simplisafe:keychain_remote:U9K-KR1 cpe:2.3:h:simplisafe:keychain_remote:U9KR2 cpe:2.3:h:simplisafe:carbon_monoxide:U9K-CO1000 cpe:2.3:h:simplisafe:entry_sensor:U9K-ES1000 cpe:2.3:h:simplisafe:freeze_sensor:U9K-FS1000 cpe:2.3:h:simplisafe:glassbreak_sensor:U9K-GB1000 cpe:2.3:h:simplisafe:motion_sensor:U9K-MS1000 cpe:2.3:h:simplisafe:panic_button:U9K-PB1000 cpe:2.3:h:simplisafe:smoke_detector:U9KSD1000 cpe:2.3:h:simplisafe:water_sensor:U9K-WT1000	Base Station, Keypad, Keychain Remote, and Sensors.
Attack Theater : Limited Remote Limited Remote Type : Wireless	Attacker must be within radio range (15-30m) to execute attack using RTL-SDR Dongle.
Context : Firmware	*Context* with recognized impacts due to the vulnerability
Entity Role : Primary Authorization Entity Role : Vulnerable	*Context* is the only authorization scope
Impact Method : Trust Failure Trust Failure Type : Failure of Inherent Trust Impact Method : Authentication Bypass Impact Method : Man-in-the-Middle	
Logical Impact : Read (Direct) Scope : Limited Criticality : High Logical Impact : Write (Direct) Scope : Limited Criticality : High Logical Impact : Service Interrupt Service Interrupt Type : Hang Scope : Unlimited Criticality : High	Attacker is able to decode transmitted packets, replay transmitted packets (including PIN sequences) with or without fully decoding them. SimpliSafe Original Home Security System customers may subscribe to a SimpliSafe service that provides SMS and email notifications of DISARM events.

Scenario 2

<table>
<tr><td colspan="2">Vulnerability : cve.mitre.org CVE-2018-11401</td></tr>
<tr><td colspan="2">Provenance : https://ioactive.com/pdfs/IOActive_Advisory_SimpliSafe-Replay.pdf; https://greatscottgadgets.com/2016/02-19-low-cost-simplisafe-attacks/; https://www.simpleorsecure.net/simplisafe-security-advisory/</td></tr>
<tr><td>Scenario : 2</td><td>The second scenario</td></tr>
<tr><td>Product :
cpe.nist.gov
cpe:2.3:h:simplisafe:base_station:U9K-BS1000
cpe:2.3:h:simplisafe:base_station:U9K-BS2000
cpe:2.3:h:simplisafe:keypad:U9K-KP1000
cpe:2.3:h:simplisafe:keychain_remote:U9K-KR1
cpe:2.3:h:simplisafe:keychain_remote:U9KR2
cpe:2.3:h:simplisafe:carbon_monoxide:U9K-CO1000
cpe:2.3:h:simplisafe:entry_sensor:U9K-ES1000
cpe:2.3:h:simplisafe:freeze_sensor:U9K-FS1000
cpe:2.3:h:simplisafe:glassbreak_sensor:U9K-GB1000
cpe:2.3:h:simplisafe:motion_sensor:U9K-MS1000
cpe:2.3:h:simplisafe:panic_button:U9K-PB1000
cpe:2.3:h:simplisafe:smoke_detector:U9KSD1000
cpe:2.3:h:simplisafe:water_sensor:U9K-WT1000</td><td>SimpliSafe Original Home Security System Base Station, Keypad, Keychain Remote, and Sensors.</td></tr>
<tr><td>Attack Theater : Limited Remote
Limited Remote Type : Wireless

Barrier : Environmental Condition
Privilege Level : Anonymous
Relating to Context : Firmware</td><td>Attacker must be proximate to an installed SimpliSafe Original Home Security System. This attack requires signal broadcast functionality and cannot be executed with an RTL-SDR Dongle or other receive-only device. Anecdotally, this attack has been successfully executed against a SimpliSafe Original Home Security System using a handheld Baofeng HAM radio transmitting at 433.92MHz, creating sufficient RF noise to drown out Wireless Keypad, Keychain Remote, and Sensor transmissions to the Base Station of the SimpliSafe Original</td></tr>
</table>

	Home Security System, thus disabling the system.
Context : Firmware	*Context* with recognized impacts due to the vulnerability
Entity Role : Primary Authorization Entity Role : Vulnerable	*Context* is the only authorization scope
Impact Method : Trust Failure Trust Failure Type : Failure of Inherent Trust Impact Method : Authentication Bypass Impact Method : Man-in-the-Middle	
Logical Impact : Read (Direct) Scope : Limited Criticality : High Logical Impact : Write (Direct) Scope : Limited Criticality : High Logical Impact : Service Interrupt Service Interrupt Type : Hang Scope : Unlimited Criticality : High	Attacker is able to introduce RF interference which may affect the efficacy of Sensor or Keypad transmissions to the Base Station of the SimpliSafe Original Home Security System.

Scenario 3

Vulnerability : cve.mitre.org CVE-2018-11400	
Provenance : https://youtu.be/wkRQTRVxK4g; https://www.simpleorsecure.net/simplisafe-security-advisory/	
Scenario : 3	The third scenario
Product : cpe.nist.gov cpe:2.3:h:simplisafe:base_station:U9K-BS1000 cpe:2.3:h:simplisafe:base_station:U9K-BS2000	SimpliSafe Original Home Security System Base Station.
Attack Theater : Physical	Attacker must have physical access to the Base Station; physical access must be achieved and the disarming attack must

Barrier : Precondition Required Privilege Level : Anonymous Relating to Context : Firmware	be executed before an alarm is sent (i.e., within the "entry delay" window, default is 30 seconds, but timing is configurable)
Context : Firmware Context : Application	*Context* with recognized impacts due to the vulnerability
Entity Role : Vulnerable	*Context* contains the vulnerability
Impact Method : Trust Failure Trust Failure Type : Failure of Inherent Trust	
Logical Impact : Service Interrupt Service Interrupt Type : Shutdown Scope : Unlimited Criticality : High	Attackers with physical access to a SimpliSafe Original Home Security System Base Station may disable the system by removing the Base Station battery and disconnecting the external power supply. This action interrupts cellular communications among associated Sensors, Wireless Keypads, Keychain Remotes and the Base Station of the SimpliSafe Original Home Security System, and halts all outgoing transmissions from the Base Station. Removal of the Base Station battery and external power supply may be accomplished by an attacker within the "entry delay" window (default is 30 seconds, but timing is configurable) if an attacker has knowledge regarding the location of the Base Station.

Remediation

SimpliSafe issued several recommendations in a blog post responding to initial disclosures by IOActive researchers in 2016.[5] [6] This advisory supplements prior guidance and supersedes any prior conflicts.

[5] IOActive Security Advisory, 'Replay Attack in SimpliSafe Alarm System,' 17 February 2016.
[6] SimpliSafe blog, 'Our Commitment to Your Safety,' 19 February 2016.

SimpliSafe Original Home Security System Initial Guidance	SimpliSafe Original Home Security System Updated Guidance
Change your PIN code regularly. This is a good security practice regardless.	*Change your PIN code if you know or suspect it has been compromised. Choose a robust but memorable PIN and keep it safe. Avoid sequential, quad, birth year, and other common PIN formulations (e.g., 4567, 3333, 1989).* Frequent PIN code changes theoretically shorten the period of time during which it may be captured or observed, then replayed or entered manually to a targeted system's keypad. However, a manual PIN change would only protect against these attacks if it occurred in the interval between PIN capture (which is not detectable) and replay or entry into a target system. In line with current guidelines published by the National Institute of Standards and Technology (NIST), SimpliSafe does not recommend that customers rotate PIN codes in the absence of evidence or suspicion of compromise.[7]
Monitor notifications of your alarm being disarmed for any unexpected activity.	*Monitor notifications of your alarm being disarmed for any unexpected activity.* DISARM alerts are transmitted via SMS and email to customers who pay for the SimpliSafe® Interactive monitoring service. These notifications are not available to users of the SimpliSafe Original Home Security System on the Standard monitoring plan.
Take note of any suspicious person or unidentified equipment located very near to	*As always, be aware of normal activity in the area around your home and take note of any*

[7] US Department of Commerce, NIST SP 800-63b, 'Digital Identity Guidelines: Authentication and Lifecycle Management, p. 14.

your home as you come and go, as the concern raised requires close proximity.	*suspicious persons or unidentified equipment in the near vicinity.* While remaining alert and observant is excellent practice, excessive vigilance confers marginal benefit. Given more expensive and more powerful equipment than that used to validate attacks described in this advisory, Great Scott Gadgets estimated a 1.5km range for viable PIN replay attacks.[8] In contrast, the verified attack range of ~15m still assumes optimal conditions and a minimum of interference from building structures, terrain, trees, etc. Customers of the SimpliSafe Original Home Security System in higher population density areas are not expected to observe persons and equipment inside of neighboring apartments, condos, or houses. Likewise, customers in rural areas are not expected to maintain an exclusion zone around their property. Additionally, SimpliSafe recommends keeping the Base Station out of view so that it cannot be easily found and disabled by an attacker in the home. Customers can also either configure their "entry delay" to instantly trigger an alarm, or call SimpliSafe's customer support to decrease their "entry delay" to less than 30 seconds.
If you have our Interactive plan, disarm your system with your smartphone or web app, which bypasses this issue.	*If you have our Interactive plan, disarm your system with your smartphone or web app, which bypasses this issue.* This mitigation requires users of the SimpliSafe Original Home Security System to be enrolled in the Interactive monitoring

[8] Michael Ossmann, 'Low Cost SimpliSafe Attacks,' *Great Scott Gadgets Blog*, 20 February 2016.

	plan. This mitigation does not apply to users enrolled in the Standard monitoring plan.

References

[1] IOActive, 'Replay Attack in SimpliSafe Alarm System,' IOActive Security Advisory, 17 February 2016. https://web.archive.org/web/20170610212530/https://ioactive.com/pdfs/IOActive_Advisory_SimpliSafe-Replay.pdf

[2] Thomas Fox-Brewster, '300,000 American Homes Open to Hacks of "Unfixable" SimpliSafe Alarms,' *Forbes*, 17 February 2016. https://www.forbes.com/sites/thomasbrewster/2016/02/17/simplisafe-alarm-attacks/#771b3df13b00

[3] SimpliSafe™ , 'Our Commitment to Your Safety,' *SimpliSafe Blog*, 19 February 2016. https://web.archive.org/web/20170911205125/http://simplisafe.com/blog/our-commitment-to-your-security

[4] Michael Ossmann, 'Low Cost SimpliSafe Attacks,' *Great Scott Gadgets Blog*, 20 February 2016. https://web.archive.org/web/20180111053329/https://greatscottgadgets.com/2016/02-19-low-cost-simplisafe-attacks/

[5] CVE-2017-19710 — Hoermann BiSecur devices.[9] [10]

[6] Adam Callis, 'SimpliSafe Security Advisory,' *Simple or Secure Security Blog*, 17 May 2018. https://web.archive.org/web/20180604145548/https://www.simpleorsecure.net/simplisafe-security-advisory/

Credit

Initial disclosure by Dr. Andrew Zonenberg (IOActive) with subsequent reporting by Michael Ossmann (Great Scott Gadgets) and rtl_433 support by Adam Callis.

[9] 'On Hoermann BiSecur devices before 2018, a vulnerability can be exploited by recording a single radio transmission. An attacker can 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 use of AES-128 with an initial static random value and static data vector (all of this static information is the same across different customers' installations), 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 ("wireless cloning"). To conduct the attack, a low cost Software Defined Radio (SDR) is sufficient. This affects Hoermann Hand Transmitter HS5-868-BS, HSE1-868-BS, and HSE2-868-BS devices.' https://nvd.nist.gov/vuln/detail/CVE-2017-17910.

[10] Trustworks KG Security Advisory, 'Predictable AES-128 key, wireless cloning,' 04 October 2017, https://docs.wixstatic.com/ugd/28ba71_6ecc3158975a484d827e935edda4fa17.pdf.

Contact Information - security@simplisafe.com

Terms of Use - https://simplisafe.com/legal

This advisory is based upon information available to SimpliSafe as of the date of this report and SimpliSafe's good-faith understanding of all relevant facts and circumstances associated with the matters described herein, which have been researched and examined by SimpliSafe's third-party security firm. SimpliSafe reserves all rights and defenses available under contract and law.

Disclosure Timeline

2018-01-10	SimpliSafe announces third generation product, 'All New SimpliSafe'
2018-03-21	Researcher Adam Callis contacts vendor with a security advisory describing 'Wireless Capture and Decoding of SimpliSafe Original Security Systems.'
2018-03-21	SimplISafe contacts third-party security firm for disclosure and validation assistance.
2018-03-21	SimpliSafe responds to researcher acknowledging report and indicating that vendor will follow up within a few weeks.
2018-04-03	Third-party security firm starts to reproduce and validate vulnerabilities in security advisory
2018-04-24	Researcher, SimpliSafe, and Third-Party Security Firm meet. Third-party security firm unable to reproduce the exact setup Mr. Callis used for some vulnerabilities using the limited information in security advisory.
2018-04-27	Third-party security firm reproduces all reported vulnerabilities in security advisory. Mr. Callis was informed that SimpliSafe will work towards an updated public disclosure and options for upgrades for users of the SimpliSafe Original Home Security System.

2018-05-09	SimpliSafe updated Mr. Callis on progress, and set the expectation that it will take several weeks for an update on consumer upgrade paths, given the need for marketing and finance approval on the policy.
2018-05-15	Mr. Callis presents his findings at an internal Cisco security meeting.
2018-05-24	Mr. Callis advises SimpliSafe that he has made the advisory public on https://www.simpleorsecure.net and released public code. SimpliSafe was not advised ahead of time of this planned release or timeline.
2018-08-20	SimpliSafe releases comprehensive security advisory.