Talos Vulnerability Report

TALOS-2021-1431

Swift Sensors Gateway device password generation authentication bypass vulnerability

FEBRUARY 28, 2022

CVE NUMBER

CVE-2021-40422

Summary

An authentication bypass vulnerability exists in the device password generation functionality of Swift Sensors Gateway SG3-1010. A specially-crafted network request can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability.

Tested Versions

Swift Sensors Gateway SG3-1010

Product URLs

Swift Sensors Gateway - https://www.swiftsensors.com/catalog/gateways/sg3-1010/

CVSSv3 Score

10.0 - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CWE

CWE-798 - Use of Hard-coded Credentials

Details

The Swift Sensors Gateway 1010 connects with all Series 3 Swift Sensors within range and securely transmits sensor data to the Swift Sensors Cloud through either Wi-Fi, Ethernet or Cellular (Swift Sensors Cellular Network Module Required).

While typical installation and usage does not require a user to login to the device itself, a `SSH` service can be found running on the device by default. This service is not required for standard operation and is not mentioned in the provided documentation, nor are any sort of login credentials.

However, upon analysis of the device firmware, we were able to determine their unique password generation mechanism for each device. This password is based off of the exposed `Gateway ID` printed boldly on the front of each gateway. This ID consists of 8 alphanumeric characters that are used in a substitution & encoding process that is eventually AES encrypted and base64 encoded. The base64 encoded value along with the username `pi` (this is a Raspberry Pi device with a customized 'HAT' for receiving sensor data), allows any user on the network (or if the gateway is exposed to the internet) that knows or can see the printed `Gateway ID` to login to the device using the exposed `SSH` service. From there, a user can `sudo su` straight to the `root` user.

Also of note is that the device ID and password combination is used by the Swift Sensor bridge software itself to login to the backend to report sensor data. This could potentially allow a remote user to manipulate data and/or disable sensor reporting altogether. Additionally, our research indicates that only the last 4 characters differ between bridge IDs using only capital letters and/or numbers. This small keyspace (36^4) means that an attacker could in theory, brute-force each possible device ID and password combination to login to the backend sensor data endpoint as those devices.This is particularly critical considering the sensor package we were sold is designed specifically for monitoring Moderna vaccine equipment.

Exploit Proof of Concept

$ ssh pi@192.168.1.223 pi@192.168.1.223's password: Linux WBERN3-01-AYM6LWFB 5.4.81-v7l+ #1378 SMP Mon Dec 7 18:43:09 GMT 2020 armv7l

The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Last login: Mon Nov 29 15:51:43 2021 from 192.168.1.224 pi@WBERN3-01-AYM6LWFB:~$ sudo su root@WBERN3-01-AYM6LWFB:/home/pi# whoami root root@WBERN3-01-AYM6LWFB:/home/pi# uname -a Linux WBERN3-01-AYM6LWFB 5.4.81-v7l+ #1378 SMP Mon Dec 7 18:43:09 GMT 2020 armv7l GNU/Linux root@WBERN3-01-AYM6LWFB:/home/pi#

Timeline

2021-12-14 - Vendor disclosure
2021-12-14 - Initial vendor contact
2022-02-02 - Vendor patched
2022-02-28 - Public Release

CREDIT

Discovered by Dave McDaniel of Cisco Talos.
