Issued 3/24/17

Burglars Can Easily Make Google Nest Security Cameras Stop Recording

The vulnerabilities are present in the latest firmware version running on the devices (v5.2.1). They were discovered by researcher Jason Doyle last fall, and their existence responsibly disclosed to Google, but have still not been patched.

The first two flaws can be triggered and lead to a buffer overflow condition if the attacker sends to the camera a too-long Wi-Fi SSID parameter or a long encrypted password parameter, respectively. That's easy to do as Bluetooth is never disabled after the initial setup of the cameras, and attackers (e.g. burglars) can usually come close enough to them to perform the attack. Triggering one of these flaws will make the devices crash and reboot.

The third flaw is a bit more serious, as it allows the attacker to force the camera to temporarily disconnect from the wireless network to which it is connected by supplying it a new SSID to connect to. If that particular SSID does not exist, the camera drops its attempt to associate with it and return to the original Wi-Fi network, but the whole process can last from 60 to 90 seconds, during which the camera won't be recording.

Doyle has released PoC exploits for each flaw. Unfortunately, Bluetooth can't be disabled on these cameras, so there is little users can do to minimize this particular risk. Nest has apparently already prepared a patch

but hasn’t pushed it out yet. It is supposedly scheduled to be released soon, but no date has been posted.