

IoT Robot Vacuum Vulnerabilities Let Hackers Spy on Victims

Author: Lindsey O'Donnell, July 19, 2018 2:55 pm

Two vulnerabilities were discovered on Dongguan Diqee-branded vacuum cleaners, Thursday.

UPDATE

Researchers have uncovered vulnerabilities in a connected vacuum cleaner lineup that could allow attackers to eavesdrop, perform video surveillance and steal private data from victims.

Two vulnerabilities were discovered in Dongguan Diqee 360 vacuum cleaners, which tout Wi-Fi capabilities, a webcam with night vision, and smartphone-controlled navigation controls. These would allow control over the device as well as the ability to intercept data on a home Wi-Fi network.

“Like any other IoT device, these robot vacuum cleaners could be marshaled into a botnet for DDoS attacks, but that’s not even the worst-case scenario, at least for owners,” Leigh-Anne Galloway, cybersecurity resilience lead at Positive Technologies, said on Thursday.

The first bug (CVE-2018-10987) is a remote code execution issue that resides in the REQUEST_SET_WIFIPASSWD function (UDP command 153) of the vacuum.

“This vulnerability allows attackers to obtain superuser rights on the vacuum, meaning they can control it remotely, viewing video and images, and physically moving the vacuum,” Galloway told Threatpost. “It can also be used in a botnet for DDoS attacks or for bitcoin mining.”

An attacker can discover the vacuum on the network by obtaining its media access control (MAC) address – an unique identifier assigned for communications at the data link layer of a network.

They can then send a specially-crafted user datagram communications protocol (UDP) request, which results in execution of a command with superuser rights on the vacuum. A crafted UDP packet runs “/mnt/skyeye/mode_switch.sh %s” with an attacker controlling the %s variable.

“To succeed, the attacker must authenticate on the device—which is made easier by the fact that many affected devices have the default username and password combination (admin:888888),” researchers said.

A second vulnerability (CVE-2018-10988) would also allow superuser rights, but additionally, could enable crooks to steal unencrypted data, including photos, video and emails, sent from other devices on the same Wi-Fi network.

The bug exists in the vacuum’s update mechanism – and it is less threatening as it requires attackers to have physical access to the vacuum. Attackers exploiting this bug could create a special script and place it on a microSD card, then insert it into the vacuum.

After the card is inserted, the vacuum update system runs firmware files from the upgrade_360 folder with superuser rights, without any digital signature check. The script could run arbitrary code, such as a sniffer, to intercept private data sent over Wi-Fi by other devices.

Positive Technologies told Threatpost it followed responsible disclosure practices, alerting the company on March 15, 2018. Positive Technologies also submitted the vulnerabilities officially (CVE-2018-10987 and CVE-2018-10987).

“Positive Technologies does not have any information about whether or not the vulnerabilities have been fixed to date,” the company told Threatpost.

A spokesperson with Chinese supplier Dongguan Diqee did not specify whether a patch was issued, but said end users should change their default usernames and passwords.

“[It’s a] default username and password problem, users can bind the device once they receive it and modify the password immediately after binding [is] completed and prevent others from listening with the default username and password,” the spokesperson said. “After modification, the default username and password are not effective.”

A similar incident occurred last year, when researchers discovered that LG’s Hom-Bot IoT vacuum cleaner lineup was open to a hack that would let an attacker take control of the devices and their cameras –and give them the ability to live-stream video from inside a home.

These vulnerabilities may also affect other IoT devices using the same video modules as Dongguan Diqee 360 vacuum cleaners. Such devices include outdoor surveillance cameras, DVRs, and smart doorbells, researchers said.

“New IoT devices are being created and deployed every day,” Galloway told Threatpost. “If these issues continue to go addressed, IoT security will progressively get worse. To address security issues, the industry should create a comprehensive, agreed-upon set of guidelines in cooperation with all parties, from hardware manufacturers to service providers and security experts.”