Segway/Ninebot MiniPRO: Company addresses some security issues

July 21 2017, by Nancy Owano

(Tech Xplore)—Here it is July 2017 and security vulnerability stories keep coming in with the word "firmware" as one of the key words. What's up this time?

Segway/Ninebot MiniPRO was found by security researchers from IOActive Labs able to be hacked and controlled remotely.

Meanwhile, IOActive disclosed the vulnerabilities to Segway/Ninebot. The company responded. It has released a new version to address some of the issues identified, reported IOActive on Wednesday, and informed IOActive of the fixes.

"The good news," said Lily Newman in *Wired*, is that IOActive disclosed the bugs in January and "the company addressed the bulk of the problems in an app update in April."

If you are not familiar with this Segway MiniPRO, Segway had introduced features for its version of a hoverboard called the MiniPRO, said Alfred Ng in CNET, that let you connect the self-balancing scooter to your phone through Bluetooth and control the machine remotely through an app.

The Labs put out a video explaining how the vulnerabilities were wirelessly exploitable. The Labs team set up scenes to show what can happen via different types of attacks.

Thomas Kilbride, security researcher, Android developer:

"When I started looking further, I learned that regulations now require

hoverboards to meet certain mechanical and electrical specifications with the goal of preventing battery fires and various mechanical failures; however, there are currently no regulations aimed at ensuring firmware integrity and validation, even though firmware is also integral to the safety of the system."

Naked Security by Sophos said the researchers discovered that one oversight about MiniPRO was that every MiniPRO had the same PIN code.

But let Thomas Kilbride, explain, in a blog on the IOActive site:

"Using protocol analysis, I determined I didn't need to use a rider's PIN (Personal Identification Number) to establish a connection. Even though the rider could set a PIN, the hoverboard did not actually change its default pin of '000000.'"

He connected over Bluetooth while bypassing security controls.

Regarding the application, he said in the video that with it he could bypass safety mechanisms—wait, let us zoom in on how this looks: he said the attacker could remotely disable motors while the rider was in motion.

Also, in one scene, the device was shown locking up and then subsequently running away. In other words, the attacker was able to shut them down but also to drive them off.

Bugs in turn could be weaponized.

The video said the "find riders nearby" feature exposes the location of riders nearby. In his blog, he said he determined that connected riders in the area were indexed using their phones' GPS; therefore, he said, each

rider's location is published and publicly available.

Among Kilbride's recommendations for manufacturers: Use Bluetooth authentication; encrypt firmware. And check the firmware for authenticity—before being applied.

Also, hide the location of a rider from public viewing. This could prevent an attacker from easily weaponizing an exploit like his.

Advice for consumers? Kilbride said to avoid any remote functionality that is not necessary and stay current with updates

In the Wednesday press release from IOActive: "IOActive disclosed the vulnerabilities to Segway/Ninebot, and the company subsequently released a new version to address some of the issues identified and informed IOActive of the fixes."

More information: www.ioactive.com/news-events/i … ipro-hoverboard.html
blog.ioactive.com/2017/07/mult … abilities-found.html