Wemo won’t fix Smart Plug vulnerability allowing remote operation

Enlarge / This guy? This guy can be tricked into offering remote control if you give it a long name. But he’s too old for his maker to care much about that.

reader comments

66 with

I once co-owned a coworking space. The space had doors with magnetic locks, unlocked by a powered relay. My partners and I realized that, if we could switch power to the system on and off, we could remotely control the door lock. One of us had a first-generation Wemo plug, so we hooked that up, and then the programmer among us set up a script that, passing Python commands over the local network, switched the door lock open and closed.

Sometimes it would occur to me that it was kind of weird that, without authentication, you could just shout Python commands at a Wemo and it would toggle. I’m having the same feeling today about a device that’s one generation newer and yet also possesses fatal flaws.

IoT security research firm Sternum has discovered (and disclosed) a buffer overflow vulnerability in the Wemo Mini Smart Plug V2. The firm’s blog post is full of interesting details about how this device works (and doesn’t), but a key takeaway is that you can predictably trigger a buffer overflow by passing the device a name longer than its 30-character

limit—a limit enforced solely by Wemo's own apps—with third-party tools. Inside that overflow you could inject operable code. If your Wemo is connected to the wider Internet, it could be compromised remotely.

The other key takeaway is that Wemo-maker Belkin told Sternum that it would not be patching this flaw because the Mini Smart Plug V2 is "at the end of its life and, as a result, the vulnerability will not be addressed." We've reached out to Belkin to ask if it has comments or updates. Sternum states that it notified Belkin on January 9, received a response on February 22, and disclosed the vulnerability on March 14.

Advertisement

Sternum suggests avoiding the exposure of any of these units to the wider Internet, segmenting it into a subnet away from sensitive devices, if possible. A vulnerability could be triggered through Wemo's cloud-based interface, however.

The community app that makes the vulnerability possible is pyWeMo (an updated fork of the version used at my coworking space). Newer Wemo devices offer more features, but they still respond to network commands sent from pyWeMo without any password or authentication.

Belkin's Wemo devices have caused smart home security headaches before. In February 2014, security researchers revealed that its devices leaked passwords through a firmware update workflow; Belkin said it had already patched the issues in a firmware update, though it seemingly told neither the original reporting researcher nor US-CERT (now Cybersecurity and Infrastructure Security Agency). In 2019, researchers reported that a vulnerability reported one year prior to Belkin was still an issue.

Wemo's vulnerable plugs were some of the most popular and simple available, recommended by many smart home guides and seemingly purchased by thousands of buyers, based on reviews.

While they debuted in 2019, they’re not smartphones or tablets. Four years later, people didn’t have a good reason to get rid of them until now.

I have a couple at my home that do mundane things like “toggle the string lights on my banister on at sunset and off at 10 pm” and “turn on the white noise machine when I’m too lazy to get up from bed to do that.” They will be secure from remote code executions once they have been shredded and sorted into component metals by my regional e-waste facility.

One thing that would help Wemo’s devices escape their Internet-exposed vulnerabilities and end-of-life support shortfalls would be offering local-only support through Matter. Belkin, however, is not eager to jump into Matter support just yet, saying it may offer it in its Wemo products once it can “find a way to differentiate them.” One might suggest that Belkin has now been presented with at least one notable way its future products could be different.

https://arstechnica.com/?p=1939645