Amazon has mitigations so that Alexa does not turn into eavesdropper

April 27 2018, by Nancy Owano

Credit: CC0 Public Domain

Amazon has fixed a potential exploit discovered by Checkmarx. The latter's researchers said that Alexa could possibly keep tabs on you even if you were totally unaware that malicious outsiders were turning your

Echo into a listening device. The lab sleuths discovered a way to keep Amazon's voice assistant constantly listening.

Alfred Ng in CNET said "Amazon said it's since fixed the reported issues." For example, Ng reported, Amazon removed the ability to silence reprompts, and it shortened the amount of time Alexa could listen for.

Checkmarx described what was going on. "For the Echo, similar to the Google Home with voice assistant, listening is key. The device is continuously listening to catch you say its wake word (e.g. 'Alexa'), so that it can give you what you need instantly," said Checkmarx.

But researchers got curious. Could Echo record a user without the user being aware of being recorded? Could this be a silent eavesdropper, serving as a tapping device?

"Amazon Echo (with its virtual assistant known as Alexa) is the most sold Intelligent Personal Assistant (IPA) ever, with over 31 million devices sold to date," said Checkmarx. "However, with its rise in popularity, one of the main concerns with IPAs is privacy," and they noted concerns included the fear of unknowingly being recorded.

Maty Siman and Shimi Eshkenazi worked in the Checkmarx lab to see what could happen if they attempted to turn their Amazon Echo into a tapping device.

Wired reflected how they did not even have to get involved with hacking the voice assistant to turn it into a spy; eavesdropping came from just some clever coding.

Lily Hay Newman wrote about how they worked it out. She said the researchers created "a malicious Alexa applet—known as a 'skill'—that

could be uploaded to Amazon's Skill Store."

(But what is Skill? Ng explained that Alexa uses Skills to carry out commands. "You ask if rain is coming, for example, and Alexa uses the 'Weather' Skill to answer.")

Newman wrote, "To use a skill, you have to say your device's wake word for the mic to begin shuttling audio over the internet for processing. In Checkmarx's example, when the user then asks their enabled calculator to do some simple math, that request gets routed to the skill, which returns the answer."

That's where things got interesting. Though the interaction would end there, and the mic would stop transmitting, the team programmed the skill so that "a developer functionality called 'shouldEndSession' would automatically keep the Echo listening for another cycle." And, with further moves on the part of the researchers, they found the Echo would stay quiet and not let a user know the session was continuing.

Checkmarx told Amazon about their attack scenario and Amazon listened (no sarcasm intended).

Checkmarx listed some of the measures that were put in place: Setting specific criteria to identify (and reject if necessary) eavesdropping skills during certification; detecting empty-reprompts and taking appropriate actions; detecting longer-than-usual sessions and taking appropriate actions.

Ng in CNET: Checkmarx said Amazon's fixes made it impossible to repeat the same eavesdropping tactic. As for Amazon's reaction, carried in *Wired*: A company spokesperson in a statement said that, "We have put mitigations in place for detecting this type of skill behavior and reject or suppress those skills when we do."

More information: www.checkmarx.com/2018/04/25/e … g-with-amazon-alexa/

Citation: Amazon has mitigations so that Alexa does not turn into eavesdropper (2018, April 27) retrieved 10 April 2024 from https://techxplore.com/news/2018-04-amazon-mitigations-alexa-eavesdropper.html