Amazon Alexa bug exposed voice data

August 14 2020, by Peter Grad

Credit: Pixabay/CC0 Public Domain

"Alexa, who is hacking into my system?"

More than 200 million Amazon Echo, Dot and Show owners probably won't get an answer from the popular personal assistants, but it's a question they may begin asking themselves.

Researchers at security firm Check Point reported Thursday they found a bug that would permit hackers to obtain voice history data and install Alexa skills or Google actions without the user's knowledge. This means conversations users have with Alexa concerning personal data could be obtained and used to infiltrate their Amazon devices.

Check Point explained that once personal data was obtained, a hacker could pose as a legitimate user, delete an installed skill and substitute it with a doctored version containing malicious code. In turn, once the contaminated program is activated, a hacker could obtain sensitive user data by eavesdropping on conversations. Such information could involve financial transactions, health details or exchanges of a personal nature a user may engage in through Amazon inquiries.

One approach a hacker could use is to create a legitimate-looking link to a site used for tracking Amazon packages. An unsuspecting user clicking on the link will provide an entranceway for the hacker to swap installed skills with malicious ones.

"Smart speakers and virtual assistants are so commonplace that it's easy to overlook just how much personal data they hold, and their role in controlling other smart devices in our homes," said Oded Vanunu, Check Point's head of products vulnerabilities research. "But hackers see them as entry points into people's lives, giving them the opportunity to access data, eavesdrop on conversations or conduct other malicious actions without the owner being aware. We conducted this research to highlight how securing these devices is critical to maintaining users' privacy."

Amazon said it has patched the vulnerabilities and expressed doubt that any actual breaches had occurred. Banking information, such as balances, are redacted from Alexa's logs, Amazon added.

Check Point acknowledged that Amazon does not record banking login

credentials, and it emphasized that all apps, or skills, in the Amazon store are screened for potentially malicious behavior. But Check Point noted that interactions are recorded, including banking tasks, so some data is potentially compromised. Referring to its research results, Check Point said, "We can also get usernames and phone numbers, depending on the skills installed on the user's Alexa account."

Meanwhile, an Amazon spokesman said, "We are not aware of any cases of this vulnerability being used against our customers or of any customer information being exposed."

Amazon by default keeps records of voice transactions with Echo devices as part of its artificial intelligence efforts. Amazon workers also may listen in to those exchanges. Users may choose to deny access to those conversations through the Alexa app. In addition, users can set Echo to delete the voice history automatically every three or 18 months. Those desiring more frequent erasures may do so manually, each day or week.

It should be noted that Amazon has reported that it keeps transcripts of some conversations even after audio has been deleted.

More information: research.checkpoint.com/2020/amazons-alexa-hacked/