

Wyze server leak exposes customer data of 2.4 million users

An unsecured server exposed the data of Wyze customers over a period of three weeks, the smart security camera manufacturer has admitted. The leak was first discovered by the cybersecurity firm Twelve Security, which published its findings on December 26th, while *IPVM*, a blog focused on video surveillance products, was able to verify that its own data had been affected by the leak. According to Twelve Security, the data of around 2.4 million Wyze customers was compromised.

In a forum post announcing the leak to its users, Wyze co-founder Dongsheng Song wrote that the exposed server was not a production server, but was instead a “flexible database” that was created to allow for customer data to be more quickly queried. The co-founder said that an employee error led to the server’s security protocols being removed on December 4th, and the data was exposed until December 26th when the company was made aware of the problem.

“We’ve always taken security very seriously, and we’re devastated that we let our users down like this”

In its blog post on the leak, Twelve Security said that the server included information like usernames, email addresses, camera nicknames, device models, firmware information, Wi-Fi SSID details, API tokens for iOS and Android, and Alexa tokens from users who’d connected Amazon’s voice assistant with their security cameras. (Wyze says that the database did not include user passwords.) The cybersecurity firm also claimed that the database included a huge array of health information, including height, weight, bone density, and daily protein

intake. Song confirmed that some health information was present thanks to a beta test of a new smart scale product, but disputed that it had ever collected information on bone density and daily protein intake.

Twelve Security even claimed that there were “clear indications” that the data was being sent to the Alibaba Cloud in China. Song’s forum post disputes this. He said that Wyze does not use Alibaba Cloud, and that although it has employees and manufacturing partners in China, it does not share user data with any government agencies.

In response to the security lapse, Song says that Wyze has begun conducting an audit of all its servers and databases, and has discovered another unprotected database. He also said that the company is revisiting “all aspects” of its security guidelines. In the meantime, the co-founder said that Wyze users should beware of phishing attacks, and that the company has logged all its users out of their accounts and unlinked their third-party integrations to try to close the security loophole caused by the compromised API and Alexa tokens.

The data leak comes at the end of a difficult year for Wyze. The company announced a new AI-powered people detection feature back in July for its affordable security cameras, only to have the AI startup it partnered with on the feature drop out in November, casting doubt on the feature’s future. The launch of its subscription service also needed to be delayed that same month due to unspecified “critical issues.”

Song was keen to emphasize that the company’s budget prices don’t mean that it takes security any less seriously. “We’ve often heard people say, ‘You pay for what you get,’ assuming Wyze products are less secure because they are less expensive. This is not true,” the co-founder wrote. “We’ve always taken security very seriously, and we’re devastated that we let our users down like this.”

<https://www.theverge.com/2019/12/30/21042974/wyze-server-breach-cybersecurity-smart-home-security-camera>