



***Issued 3/1/17***

## **Cloudpets Toys Leak Kid, Adult User Info, Voice Recordings**

Talking toys can vacillate between creepy and cute, but sometimes they come with hidden perils—like the CloudPets - whose custom audio files allow parents and children to exchange customized messages through cuddly stuffed bears – were just found to be on a MongoDB “in a publicly facing network segment without any authentication required” (and indexed by Shodan) with some information being held for ransom, according to a blog post by Troy Hunt, author of the Have I Been Pwned? breach disclosure site. “With the great increase of IoT devices, from teddy bears like the ones connecting with CloudPets to medical devices monitoring patients to connected refrigerators, our race for innovation brings a lot of cool stuff to life in a very short time, and this will continue in the next years, as there is a potential to revolutionize the way we're living,” Ben Herzberg, security research group manager at Redwood Shores, Imperva, said in comments emailed to SC Media. “For most IoT sales the vendor is not monetizing the data, only the device itself (a single point in time purchase for minimal margin),” Philip Lieberman, president and CEO of Lieberman Software, said in emailed comments to SC Media.

Companies, though, are facing increasing pressure to bring their devices, whether stuffed bears or thermostats, up to a higher security standard. “Every company that's selling devices that connect to the internet must know that in that moment they become

a target, and will probably not have a lot of grace time before they start getting attacked,” said Herzberg.