Two newly-discovered flaws light fire under IoT security

One of the reported flaws exposed children's personal profiles -- including name, birthdate, gender, and language.

By Zack Whittaker for Zero Day February 2, 2016 -- 14:00 GMT (06:00 PST)

If the Internet of Things has taught us anything, it's that anything that's connected to the internet can be hacked.

Enter two new, previously unreported security flaws published Tuesday by security firm Rapid7 https://community.rapid7.com/community/infosec/blog/2016/02/02/security-vulnerabilities-within-fisher-price-smart-toy-hereo-gps-platform). At the center of the flaws are two internet-connected smart devices which improperly authenticated the user with the device's corresponding web service.

Fisher-Price's Smart Toy, a Wi-Fi-enabled stuffed animal, was vulnerable to a remote flaw. An attacker could trick the web service (API) to send requests that shouldn't be authorized. From there, an attacker could allow easily find all customers -- whose accounts were associated with a unique sequential integer -- and associated children's profiles, and have wide access to create, edit, or delete children's profiles on a customer's account.

Children's profiles contain names, their birthdate, gender, language, and which toys they have played with.

A popular Fisher-Price 'smart bear' failed to properly authenticate the device's user.

Image Credit: Amazon

In a blog post describing the vulnerability, security researcher Mark Stanislav said an attacker "could hijack the device's functionality and manipulate account data, they could effectively force the toy to perform actions that the child user didn't intend, interfering with normal operation of the device."

A second flaw, this time affecting HereO, a smart GPS watch (http://www.cnet.com/products/hereo-gps-watch/) designed for children, similarly took advantage of a flaw in how the watch authenticates with its web service. The flaw, which relied on tricking a family's group into accepting a request to join their group, could let an attacker have access to every family member's location and location history.

Both Fisher-Price and HereO fixed the vulnerabilities within the three-month responsible disclosure limit.

Mattel, which owns Fisher-Price, said in a statement (http://www.kb.cert.org/vuls/id/719736): "We recently learned of a security vulnerability with our Fisher-Price Wi-Fi-connected Smart Toy Bear. We have remediated the situation and have no reason to believe that customer information was accessed by any unauthorized person. Mattel and Fisher-Price take the safety of our consumers and their personal data very seriously, which is why we act quickly to resolve potential vulnerabilities like this."

Tod Beardsley, security research manager at Rapid7, told me by email that there was no evidence that the flaws were being actively exploited by attackers.

This isn't the first time the Internet of Things -- a growing number of devices that are connected to the internet -- have put users at risk. Because many of these companies put product development first and security second (http://hereO), many firms whose products are flawed are forced to patch after the fact. Security issues with internet-connected devices are so widely known, there's a search engine dedicated to finding flawed devices (https://www.zdnet.com/article/shodan-the-iot-search-engine-which-shows-us-sleeping-kids-and-how-we-throw-away-our-privacy/).

Beardsley, said that this time the companies involved were willing to fix the vulnerabilities. "That, to me, is a move in the right direction," he said.

> Following the massive cyberattack on Hong Kong-based toymaker VTech, which led to the theft of millions of children's accounts and personal data, Beardsley said some companies are starting to be more receptive towards fixing security issues.

"While I'd prefer companies spend their scarce resources on ensuring a secure design and a secure review of their various codebases, if I can just get vendors to acknowledge vulnerabilities and fix them in a timely manner, that's a huge step forward," he said.