This critical vulnerability turns home devices into attack tools

Vulnerabilities in millions of IoT devices could allow attackers to view live camera feeds, create botnets, or use the attacked device as a springboard for further attacks.

Vulnerabilities in millions of Internet of Things (IoT) devices, including security cameras, baby monitors and other digital recording devices, could allow attackers to view and listen to live data. as well as collect login information to prepare for further attacks.

Cybersecurity firm Mandiant, the Cybersecurity and Infrastructure Agency (CISA) and ThroughTek said the vulnerability appeared in IoT devices using the ThroughTek Kalay platform.

This vulnerability (codenamed CVE-2021-28372) has a CVSS of 9.6, which is classified as a critical vulnerability. Experts recommend that users upgrade to Kalay version 3.1.10 to protect devices and networks from attackers.

While Mandiant cannot aggregate all affected devices, ThroughTek figures show 83 million devices are connected through the Kalay network and there are more than 1.1 billion monthly connections to the platform.

Previously, Nozomi Networks also found security holes in ThroughTek, but the new vulnerability discovered by Mandiant is different. It allows attackers to remotely execute code on the device, take control of affected IoT devices, listen to live audio, view real-time video feeds, and compromise device credentials. to prepare for the next attack.

This is a privacy violation that seriously affects not only individual customers, especially if cameras and surveillance equipment are installed inside a private home, but also for businesses as it can monitor live. internal and private meetings.

In addition, there is also the possibility of devices being used in botnets and DDoS attacks.

"This vulnerability could potentially allow remote code execution on the attacked device, which could be used in a variety of ways, such as potentially creating a botnet from vulnerable devices or being hacked. attacks on devices that share the same network as the attacked device," said Erik Barzdukas, service manager at Mandiant.

Exploiting the CVE-2021-28372 vulnerability is very complex, requiring the attacker's time and effort. However, this did not prevent breaches from occurring, and the vulnerability is still considered critical by CISA.

Mandiant is working with vendors using the Kalay protocol to help protect devices from vulnerabilities and recommends that all IoT manufacturers and users update patches to protect devices. .