MUST WATCH: Boston Dynamics bipedal robots complete parkour obstacle course

Critical IoT security camera vulnerability allows attackers to remotely watch live video - and gain access to networks

Mandiant, CISA and ThroughTek disclose a vulnerability in millions of devices that could let attackers watch live camera feeds, create botnets or use hacked devices as a stepping stone to further attacks.

By Danny Palmer | August 17, 2021 -- 12:00 GMT (05:00 PDT) | Topic: Security

Security vulnerabilities in millions of Internet of Things (IoT) devices, including connected security cameras, smart baby monitors and other digital video recording equipment, could allow cyber attackers to compromise devices remotely, allowing them to watch and listen to live feeds, as well as compromise credentials to prepare the ground for further attacks.

The vulnerabilities in IoT devices (https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/) that use the ThroughTek Kalay network (https://www.throughtek.com/overview/) have been disclosed by cybersecurity company Mandiant (https://www.fireeye.com/blog/threat-research/2021/08/mandiant-discloses-critical-vulnerability-affecting-iot-devices.html) in coordination with the Cybersecurity and Infrastructure Security Agency (CISA) and ThroughTek.

ZDNET RECOMMENDS

Best VPN services (https://www.zdnet.com/article/best-vpn/)

Best security keys (https://www.zdnet.com/article/best-security-key/)

Best antivirus software (https://www.zdnet.com/article/best-antivirus/)

The fastest VPNs (https://www.zdnet.com/article/fastest-vpn/)

It's tracked as CVE-2021-28372 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28372) and carries a Common Vulnerability Scoring System (CVSS) score of 9.6 -- classifying it as a critical vulnerability. Upgrading to the latest version of the Kalay protocol (3.1.10) is highly recommended to protect devices and networks from attacks.

SEE: A winning strategy for cybersecurity (http://www.zdnet.com/topic/a-winning-strategy-for-cybersecurity/) **(ZDNet special report)**

While Mandiant hasn't been able to compile a comprehensive list of all the affected devices, ThroughTek's own figures suggest that 83 million connected devices are connected through the Kalay network.

Previous research by Nozomi Networks (https://www.nozominetworks.com/blog/new-iot-security-risk-throughtek-p2p-supply-chain-vulnerability/) also found vulnerabilities in ThroughTek, but the new vulnerabilities disclosed by Mandiant are separate and allow attackers to execute remote code on devices.

Researchers were able to combine dissembling ThroughTek libraries via official apps from both the Google Play Store and Apple App Store with developing a fully functional implementation of ThroughTek's Kalay protocol. This allowed key actions to be taken, including device discovery, device registration, remote client connections, authentication, and the processing of audio and video (AV) data.

By writing an interface for creating and manipulating Kalay requests and responses, researchers could identify logic and flow vulnerabilities in the Kalay protocol -- most notably, the ability to identify and register devices in a way that allows attackers to compromise them.

Attackers achieve this by obtaining a Kalay-enabled client device's uniquely assigned identifier, which can be discovered via web APIs such as mobile applications. Once they've obtained the UID of a device, they can register it, which causes Kalay servers to overwrite the existing device, directing attempts to connect to the device into the path of the attacker.

By doing this, attackers can obtain the username and password needed to access the device, which they can then use to access it remotely -- complete with the ability to monitor audio and video data in real time.

"Once an attacker obtained UIDs, they could redirect client connections to themselves and obtain authentication materials to the device. From there, an attacker could watch device video, listen to device audio, and potentially compromise the device further depending on device functionality," Erik Barzdukas, manager of proactive services at Mandiant Consulting, told ZDNet.

Not only is this a massive privacy violation for the users, particularly if the cameras and monitors are installed inside their own homes, but compromised devices in enterprise settings could allow attackers to snoop on sensitive discussions and meetings, potentially providing them with additional means of compromising networks.

There's also the potential for devices to be recruited into a botnet and used to conduct DDoS attacks (https://www.zdnet.com/article/what-is-a-ddos-attack-everything-you-need-to-know-about-ddos-attacks-and-how-to-protect-against-them/).

"This vulnerability could potentially allow for remote code execution on the victim device, which may be used maliciously in a variety of its own ways, like potentially creating a botnet out of the vulnerable devices or further attacking devices on the same network as the victim device," said Barzdukas.

Exploiting CVE-2021-28372 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28372) is complex and would require time and effort from an attacker. But that doesn't make it impossible, and the vulnerability is still considered critical by CISA.

SEE: The cybersecurity jobs crisis is getting worse, and companies are making basic mistakes with hiring (https://www.zdnet.com/article/the-cybersecurity-jobs-crisis-is-getting-worse-and-companies-are-making-basic-mistakes-with-hiring/)

Mandiant is working with vendors who use the Kalay protocol to help protect devices from the vulnerability, and recommends that no matter the manufacturer, IoT users should regularly apply patches (https://www.zdnet.com/article/this-one-change-could-protect-your-systems-from-attack-so-why-dont-more-companies-do-it/) and updates to devices to ensure they're protected against known vulnerabilities.

"Regardless of whether you own one of the impacted devices, Mandiant strongly recommends consumers and businesses with smart devices keep their devices and applications up to date," said Barzdukas.

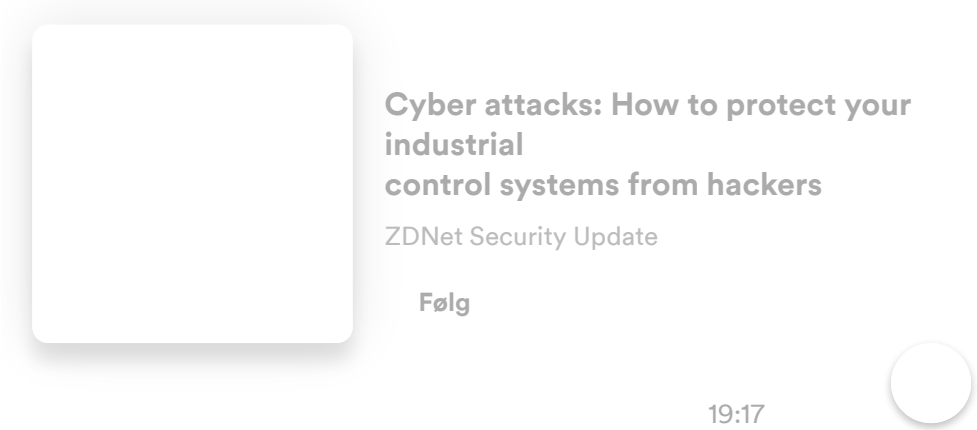
"Consumers and businesses need to set aside time -- at least once a month -- to check if their smart devices have any updates to install," he added.

"As an IoT solution provider, we are continuously upgrading sufficient software and cloud service to provide higher security mechanisms to apply in devices, connections, and client app. Although we cannot limit what API/function that developers will use in our SDK,

ThroughTek will strengthen our educational training and make sure our customers use it correctly to avoid a further security breach," a ThroughTek spokesperson told ZDNet.

"Also, we have been working with CISA to mitigate this vulnerability," they added.

Mandiant's security disclosure thanks ThroughTek -- and CISA -- "both for their cooperation and support with releasing this advisory and commitment to securing IoT devices globally."



MORE ON CYBERSECURITY

- These new vulnerabilities put millions of IoT devices at risk, so patch now (https://www.zdnet.com/article/these-new-vulnerabilities-millions-of-iot-devives-at-risk-so-patch-now/)
- IoT: Security researchers warn of vulnerabilities in hospital pneumatic tube systems (https://www.zdnet.com/article/iot-security-researchers-warn-of-vulnerabilities-in-hospital-pneumatic-tube-systems/)
- Yes, your security camera could be hacked: Here's how to stop spying eyes (https://www.cnet.com/home/security/yes-your-security-camera-could-be-hacked-heres-how-to-stop-spying-eyes/)
- Bob had a bad night: IoT mischief in a capsule hotel takes neighborly revenge to the next level (https://www.zdnet.com/article/bob-had-a-bad-night-iot-mischief-takes-neighbourly-revenge-to-the-next-level-in-a-capsule-hotel/)
- This old security vulnerability left millions of Internet of Things devices vulnerable to attacks (https://www.zdnet.com/article/this-old-security-vulnerability-left-millions-of-internet-of-things-devices-vulnerable-to-attacks/)

RELATED TOPICS: INTERNET OF THINGS | SECURITY TV | DATA MANAGEMENT | CXO | DATA CENTERS