Issued 10/11/18

World's Largest CCTV Maker Leaves at Least 9 Million Cameras Open to Public Viewing

Yet another IoT device vendor has been found to be exposing their products to attackers with basic security lapses. This time, its Chinese surveillance camera maker Xiongmai named and shamed this week by researchers with SEC Consult for the poor security in the XMEye P2P Cloud service [link]. Among the problems researchers pointed to were exposed default credentials and unsigned firmware updates that could be delivered via the service. As a result, SEC Consult warns, the cameras could be compromised to do everything from spy on their owners, to carry out botnet instructions and even to serve as an entry point for larger network intrusions. "Our recommendation is to stop using Xiongmai and Xiongmai OEM devices altogether," SEC Consult recommended. "The company has a bad security track record including its role in Mirai and various other IoT botnets. There are vulnerabilities that have been published in 2017, which are still not fixed in the most recent firmware version." Enabled by default, the P2P Cloud service allows users to remotely connect to devices via either a web browser or an iOS/Android app and control the hardware without needing a local network connection. Unfortunately, SEC Consult explained, shortcomings in both the devices themselves and the service, such as unencrypted connections and default passwords (owners are not required to change the defaults when setting up the device) mean that in many cases, accessing and compromising camera could be a cinch. Additionally, SEC Consult notes, the Xiongmai devices do not require that firmware updates be signed, meaning it would be possible for an attacker to install malware-laden firmware updates to build a botnet or stage further attacks on the local network.