Internet-Connected Baby Monitor Security Research
Frequently Asked Questions

What do I need to know?

This research project evaluated the security of nine different Internet-connected baby monitors, representing eight unique vendors, at price points between $55 and $260. As part of the assessment of these devices, we leveraged numerous techniques to evaluate individual components in each device's connected ecosystem, including assessment of mobile applications, device firmware, web services, server software, and network protocols.

During testing, numerous security weaknesses and design flaws were found, including, but not limited to:

- Hidden, hardcoded account credentials providing local (e.g. UART) and/or remote (e.g. SSH, Telnet) access
- Unencrypted video streaming from the camera locally or via a cloud service to the end-user's mobile device
- Unencrypted web and mobile application functions, including a lack of protection for API keys and credentials
- Vulnerabilities for camera services that allow a device's functionality to be maliciously abused by an attacker

After the evaluation, each device was rated on a 250-point scale for overall security functionality and implementation. The resulting scores were then graded on a standard academic scale of 'A', 'B', 'C', 'D', and 'F' to provide a fair comparison of devices to each other. Of the resulting scores, eight of the tested devices received an 'F' and one device received a 'D' when graded.

While a variety of vulnerabilities were noted during testing, three devices were found to each have a critical vulnerability impacting their overall security beyond simple weaknesses or complex-to-exploit issues:

1. The *Philips In.Sight B120* establishes a direct connection to the camera's backend web application onto the public Internet, unencrypted and unauthenticated. By brute forcing the possible hostname and port number combinations used by the third-party service provider, an attacker can locate an exposed camera and is able to watch the live stream, enable remote access (e.g. Telnet), or change the camera settings.

   It is important to note that Philips N.V. has been the most responsive of the vendors we approached with the findings of this research and is currently working on a patch that will be made available to customers. The company's vendor disclosure process is well established and clearly focused on ensuring its devices are safe for consumers. We applaud Philips' commitment to fixing this vulnerability and their established protocol for handling incoming product vulnerabilities, which included using a documented PGP key to encrypt communications around this sensitive material.

2. The *iBaby M6* has a web service issue that allows easy access to other people's camera details by changing the serial number in a URL string. By abusing this access, filenames of a camera's recorded video clips (automatically created from a motion or noise alert) can be harvested. Through a simple script, an attacker could potentially gain access to every recorded clip for every registered camera across the entire service.

3. The *Summer Infant Baby Zoom* web service contains an issue where the method of adding an authorized viewer to the camera does not require any password or secret key for access to the feed. This means that by iterating through a user identifier on a URL, an attacker can add an e-mail address of their choice to every single camera and login at will to view the stream of any camera of their choosing.

How serious is this?

The aforementioned critical vulnerabilities are of a highly serious nature for camera owners of those devices. Additional security issues, especially related to remote access protocols (e.g. SSH, Telnet) that are exposed and featuring hardcoded credentials can be risky depending on their network accessibility and a potential attacker's vantage point to that device. Each of these devices run a Linux-based operating system and thus could be a powerful point of attack for purposes other than abusing the baby monitor's intended functionality.

Which vendors/software/devices/services are affected?

The following devices were tested during the course of this research project. All listed prices reflect the price paid on Amazon.com for each device when acquired in the first half of 2015 for testing purposes.

- Gyonii (GCW-1010) - $89.34
- iBaby (M3S) - $169.95
- iBaby (M6) - $199.95
- Lens (LL-BC01W) - $54.99
- Philips (B120/37) - $77.54
- Summer (28630) - $199.99
- TRENDnet (TV-IP743SIC) - $69.99
- WiFiBaby (WFB2015) - $259.99
- Withing (WBP01) - $204.60

Who does this affect?

We tested the devices listed above, but this is not an exhaustive list, and we believe other baby monitors may be impacted by the security weaknesses, design flaws, or vulnerabilities identified through the course of this research. Firmware and software updates for these devices prior to September 2015 are likely vulnerable to the overall findings of this research.

Individual web services vulnerabilities could impact numerous devices from the same vendor and their resolution could, in many cases, be implemented seamlessly and without user intervention. Consumers should contact their camera vendor(s) to determine their individual risk related to the findings presented during the research disclosure process, including any relevant patches or software upgrades required by the end user.

On Amazon.com alone, there are 17 different connected baby monitors, but numbers around how many of these connected baby monitors have been sold are extremely hard to find. Additionally, scanning the internet to identify how many of these affected devices are online would likely violate U.S. law, so we cannot provide numbers on this.

How can the risks be mitigated or remediated?

Consumers are advised to pay attention to their individual vendors' web sites for news regarding any available firmware or mobile application updates. We advise individuals to use any camera that has not been fixed for identified issues or weaknesses sparingly – or preferably not at all – until the vendor is able to fully address the identified problems. If a baby monitor allows a password to be changed, the device owner is highly encouraged to do so and to make a strong password to protect access.

In scenarios where technically possible, device owners are encouraged to firewall network access to device network services, especially remote access protocols (e.g. SSH, Telnet) to help limit potential abuse over the Internet or shared networks of those devices.

At the time of public disclosure, we are only aware of one vendor having committed to providing a patch for the vulnerabilities. Philips has demonstrated remarkable sophistication and responsiveness in their handling of the vulnerability disclosure. They are working with their OEM partners, Gibson and Weaved, to ensure the availability of a security update in a timely manner following this disclosure.

Are these being exploited in the wild? How easy is it for attackers to take advantage of this?

In many cases, exploitation in the wild of identified security issues would have to be determined by the impacted vendors. Rapid7 is unaware of these issues being actively abused at the time of publication. Due to the broad issues identified and numerous devices involved, a singular view of ease of exploitation is not practical. However, devices with hardcoded credentials and remote access protocols (e.g. SSH, Telnet) or devices with web services impacted by vulnerabilities are at a reasonably high risk for an attacker to abuse those issues without much effort.

How did we find this? What was the timeline?

A majority of the security research process occurred during the first half of 2015. Due to the sheer number of devices assessed, specific device assessment timelines aren't readily available. All identified security issues (e.g. hardcoded credentials, vulnerabilities, etc.) were reported to the impacted vendors on July 4th, 2015. U.S. CERT was contacted 17 days later, on July 21st, 2015, to help coordinate these remediation efforts further, with general public disclosure occurring on September 2nd, 2015.

What's the broader impact?

The percentage of workers[1] who are working from home (on at least a part time basis) continues to rise across every modern economy, globally, and is increasingly common across all genders, ages, and family statuses. These employees are, as a matter of necessity, connecting to their workplace virtually, either through VPN connections or through cloud services shared by colleagues.

The presence of devices that are insecure by default, difficult to patch, and impossible to directly monitor by today's standard corporate IT security practices constitutes a threat to the IoT device and its data, and also to the network it's connected to. Attackers may be able to leverage an exposure or vulnerability to gain and maintain persistent access to an IoT device. Attackers can then use the IoT device to pivot to other devices on the network to which it's connected and traditional computers by taking advantage of the unsegmented, fully trusted nature of a typical home network.

Today, employees' home networks are rarely, if ever, "in scope" for penetration testing exercises, nor are they subject to centralized vulnerability scanners.

Another concern is the raw computing power available to attackers in the form of millions to billions of IoT devices. Many of these devices share common internal components, which, in many cases, will mean that an attack against Device X will be effective against related Device Y, and even apparently unrelated Device Z. In total, the teraflops of processing power may be effectively harnessed by malicious actors to launch powerful distributed denial of service (DDoS) attacks against arbitrary Internet targets.

Given the lack of home network and on-board monitoring, remediating such attacks may prove extremely difficult once underway, and short-term solutions will tend to deny service to large chunks of residential network space. This, in turn, can knock sizable percentages of the aforementioned stay-at-home workforce offline, with little recourse for employers not prepared to offer alternative workplace accommodations.

[1] http://www.nytimes.com/2014/03/08/your-money/when-working-in-your-pajamas-is-more-productive.html