Week 1 Initial Post

Greetings,

My name is Sean, and I’m currently majoring in Computer Science and Applied Mathematics. I have always had a general interest in software security, and I am excited to be learning more about this topic. Specifically, I have participated in some Capture the Flag (CTF) games, where you try to manipulate different systems or software on computers or within a network and as such, I hope to learn more about making my code safer through this course. Currently, I am an active-duty member of the U.S. Coast Guard, serving as a marine inspector on the West Coast, where I conduct safety and security vessel inspections for both foreign cargo vessels and our domestic fleet.

For this discussion, I chose to read the article titled ‘*2 Million IoT Devices Vulnerable to Complete Takeover’*, which highlights some significant security vulnerabilities that affected various Internet of Things (IoT) devices, including security cameras, baby monitors, and smart doorbells. The vulnerabilities in question specifically stem from a peer-to-peer (P2P) communication technology called iLnkP2P, which was developed by the organization Shenzhen Yunni Technology (O'Donnell, 2019). According to the National Institute of Standards and Technology (2019), “the algorithm used to generate device IDs (UIDs) for devices that utilize Shenzhen Yunni Technology iLnkP2P suffers from a predictability flaw that allows remote attackers to establish direct connections to arbitrary devices.”

According to O’Donnell (2019), the attack impacted over two million devices which specifically targeted brands that distributed IoT devices that utilized the P2P technology like HiChip, TENVIS, SV3C, and more, making them susceptible to vulnerability. This issue was publicly disclosed on April 24, 2019, and is actually comprised of two main vulnerabilities: one that allows attackers to discover devices online (CVE-2019-11219) and another that allows them to intercept clear text user-to-device traffic (CVE-2019-11220) (O'Donnell, 2019). Unfortunately, at the time of the article, there were no known software patches available for these vulnerabilities but there are some mitigations that one can take to help mitigate becoming a target.

To start, IoT devices, such as some of those mentioned in the article, often face several common vulnerabilities. When it comes to security measures, many IoT devices don’t require robust authentication measures, making it easier for attackers to gain access. For these devices, internet connectivity is what makes these devices work and many don’t have the built-in security like other computational devices do (Bodnar, 2024). Another example is insecure communication protocols where such devices lack proper encryption and as such, data transmitted between devices can be intercepted, such as a man-in-the-middle attack (Bodnar, 2024).

Due to these vulnerabilities, IoT devices are often subject to various hacking attempts. As with CVE-2019-11219, attackers may remotely access and hijack devices, leading to data breaches that expose video streams or even user credentials. Some IoT devices are shipped with hardcoded passwords; a function that is embedded into the device’s firmware and cannot be changed, leading to additional security vulnerabilities (Spektor, 2024). Moreover, compromised IoT devices are also exposed to being used as part of larger attacks, such as creating botnets (McMillen, 2023).

In reviewing this CVE, it is important to consider current techniques for protecting against software security attacks. To address potential security issues with IoT devices, both users and manufacturers must take action for the security of their respective devices. For users, several proactive measures can be implemented to protect against CVE-2019-11219. First, users should check the unique identifier (UID) of their devices to determine if they are among the known vulnerable ones. Additionally, blocking outbound traffic to UDP port 32100 can help prevent external access through peer-to-peer connections. If devices are found to be vulnerable, users should consider replacing them with models from reputable manufacturers that prioritize security (O'Donnell, 2019). On the vendor side, manufacturers have a responsibility to adopt strong application security practices and provide regular updates and patches to address vulnerabilities. They must also move beyond just relying on "security through obscurity" and ensure that their devices are equipped with robust security features from the outset.

In summary, this article highlights the critical need for awareness regarding IoT device security and its inherent flaws due to the overall design and product feature set. With millions of devices vulnerable to takeover through known and unknown vulnerabilities, it’s paramount for both users and manufacturers to implement practical measures to enhance overall security.

Cheers,

Sean

References

Bodnar, D. (2024, July 23). *10 IoT vulnerabilities to be aware of + protection tips*. Norton. https://us.norton.com/blog/iot/iot-vulnerabilities

McMillen, D. (2023, August 24). *Internet of Threats: IoT botnets drive surge in network attacks*. Security Intelligence. https://securityintelligence.com/posts/internet-of-threats-iot-botnets-network-attacks/

NIST. (2019, April 26). *NVD - CVE-2019-11219*. National Vulnerability Database. https://nvd.nist.gov/vuln/detail/CVE-2019-11219

O'Donnell, L. (2019, May 3). 2 million IoT devices vulnerable to complete takeover. *Threatpost*. https://threatpost.com/iot-devices-vulnerable-takeover/144167/

Spektor, H. (2024, July 28). *Top 10 IoT vulnerabilities and how to mitigate them*. Sternum IoT. https://sternumiot.com/iot-blog/top-10-iot-vulnerabilities-and-how-to-mitigate-them/