New York State Intelligence Center

Cyber Intelligence Bulletin

CAU@nysic.ny.gov
1-866-48-NYSIC (866-486-9742)

January 10, 2025 **NYSIC-CYB-25-01**

(U) Subject: Best Practices to Mitigate Threat Actor Targeting of IP Cameras

(U) Overview: Internet Protocol (IP) cameras and other Internet of Things (IoT) connected devices represent a significant vulnerability for organizations that utilize them. Their internet and network connectivity provides threat actors the opportunity to launch attacks including accessing internal networks, creating botnets, and spreading malware.[i] The exploitation of these vulnerabilities by threat actors underscores the risks posed by insufficient security measures in IoT devices.[ii] [iii] [iv] Security researchers and federal agencies have urged robust security practices, such as regular firmware updates and monitoring for unusual network activity, to mitigate the risks associated with these vulnerabilities.[v] In December of 2024, the FBI issued a notification regarding an active campaign leveraging default passwords, outdated firmware, and unoptimized configurations to gain access to Chinese-branded IP cameras and digital video recorders.[vi] The landscape of IoT device security is evolving, necessitating continuous vigilance from both manufacturers and end-users to safeguard against emerging threats.

(U) Background: IP cameras, also called network cameras, are cameras that send and receive data over the internet or local area networks (LAN). These devices are standalone with their own unique IP addresses and do not require a local recording device like traditional CCTV systems.

(U) Many IP cameras offer remote security monitoring, which requires inbound internet connections. This leaves the devices vulnerable to compromise. Open source tools like Shodan provide convenient search engines that allows users to search for vulnerable devices by brand name, port number, or software version. If a camera is compromised, the consequences can be significant for both the organization using the camera and the environment being monitored. An exploited security camera might allow unauthorized individuals to enter the location undetected, compromising physical site security. In addition, an attacker can use this device access to initiate cyber-attacks against the network infrastructure, interrupting regular operations or delivering malware.

(U) NYSIC CAU Analyst Note: Third party technologies built into IoT devices may not be maintained long-term and increase the attack surface. Customers may not be aware of such technology and therefore may not believe that certain vulnerabilities apply to their devices. Knowledge of all components included with purchased IoT products will aid in incident prevention and mitigation.

(U) Recommendations:

- Change default usernames/passwords, avoid weak credentials
  - Note that some devices may have hardcoded credentials that cannot be modified. Avoid these devices or limit outside network access
- Maintain an accurate inventory of IoT devices including vendor, model, and software versions
- Patch and update software regularly

Requirements: NY Cyber SIN 1.1, 1.2, 1.8

(U) Resources:

(U) CISA Internet of Things Security Acquisition Guidance
hxxps://www.cisa[.]gov/sites/default/files/publications/20_0204_cisa_sed_internet_of_things_acquisition_guidance_final_508_1.pdf

---

(U) For further information regarding the content of this bulletin, please contact cau@nysic.ny.gov.

(U) For general inquiries, contact the NYSIC main line at 866-48-NYSIC (866-486-9742). Report suspicious activity of a physical threat nature to 866-SAFE-NYS (866-723-3697) while utilizing 911 for emergencies.

---

[i] (U) What is IoT Device Vulnerability?; hxxps://www.fortinet[.]com/resources/cyberglossary/iot-device-vulnerabilities
[ii] (U) People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations; JCSA-20240918-001; Sep 18, 2024; hxxps://www.ic3[.]gov/CSA/2024/240918.pdf
[iii] (U) Russian Military Cyber Actors Target US and Global Critical Infrastructure; Alert Code AA24-249A; Sep 05, 2024; hxxps://www.cisa[.]gov/news-events/cybersecurity-advisories/aa24-249a
[iv] (U) Akamai: Beware the Unpatchable; Aug 28, 2024; hxxps://www.akamai[.]com/blog/security-research/2024-corona-mirai-botnet-infects-zero-day-sirt
[v] (U) IoT in Connected Communities; Oct 21, 2024; hxxps://www.cisa[.]gov/sites/default/files/2024-12/PDM24069_CCI_IoT_Device_Risk_and_Mitigation_Infographic_Final_508.pdf
[vi] (U) HiatusRAT Actors Targeting Web Cameras and DVRs; PIN 20241216-001; Dec 16, 2024; hxxps://www.ic3[.]gov/CSA/2024/241216.pdf

Please note that some of this information describes first amendment protected activities. The NYSIC recognizes that Americans have constitutionally protected rights to assemble, speak, and petition the government. The NYSIC safeguards these rights and only reports on First Amendment protected activities, although no violence or criminality has been observed, this information is provided for operational planning in the interest of assuring the safety and security of the demonstrators and the public.