Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 3, No. 3, 2023

Security Research of Webcam in the Era of Intelligent Internet of Things

Chan Chen [a], Xiaoyang Liu [b]

School of Computer Science, Yangtze University, Jingzhou, Hubei, China
[a] 1634067392@qq.com, [b] 2857911564@qq.com

Abstract: With the wide application of webcam, from only recording function to real-time call now, the camera not only brings great convenience to our life, but also protects people's property safety. But in the webcam function more and more powerful at the same time, it is also facing more security problems. From the perspective of network security, this paper analyzes the security problems faced by the camera system such as password problems, web security problems, mobile app security and the corresponding countermeasures and protection methods, which is conducive to the security construction of the camera system.

Keywords: Webcam; Network Security; Camera Vulnerability.

1. Introduction

As the camera system continues to come into our life, the camera is protecting us, but it is also facing many security threats. With the rapid development of science and technology today, the security of the camera system is also facing new opportunities and challenges. Starting from the security of the camera system, the author of this paper analyzes the security problems faced by the camera system at present, and puts forward strategies on how to improve the security of the camera system according to different people, aiming to improve the security level of the camera equipment and help the construction of network security.

2. Security Analysis of Webcam

2.1. Ignorance of the Importance of the Camera Password

The 2023 Cybersecurity Maturity Report shows that weak passwords have occupied the top spot in the rankings for the past few years, which shows that weak passwords are still a major vulnerability in network security. Especially in the camera system, on the one hand, due to the different use of people and purposes, the cognition and ideas of the importance of the camera password are also different. For example, when using the camera in the ordinary family, due to the lack of understanding of relevant professional knowledge, do not know how to set or change the password, and worry about forgetting the password, they directly use the weak password or default password. In large webcam systems, such as school camera systems and factory camera systems, due to the large number of cameras, it is difficult to configure, and if one machine one code is used, it will greatly increase the difficulty and workload of operation and maintenance, which also leads to a large number of camera weak password, default password and empty password security problems. On the other hand, due to the simple principle and simple operation method of such vulnerabilities, attackers can quickly get access to the camera as long as they request the corresponding camera through some software which can obtain the video stream, and then continue to try weak passwords and default passwords. Even if not a hacker can quickly master the principle of this vulnerability, which makes the exposure of camera security threats increase, and the probability of being attacked also increases.

2.2. Authentication Flaws

Most of the camera security vulnerabilities disclosed on CVE in recent years are about the lack of device authentication, where an attacker can construct a malicious request to gain access to the camera, such as CVE-2022-29964, CVE-2021-32934, etc. The security threat caused by the negligence in development is unpredictable. Developers who neglect the development of security functions or develop non-standard will cause a great impact.

2.3. Web Configuration Page of Webcam

In order to facilitate the configuration, each camera will open a web configuration page. However, this undoubtedly increases the probability of the camera being attacked. The login page of this configuration page often uses a weak password, including other common web vulnerabilities that may be present.

2.4. Ignorance of the Security of Webcam App

In order to facilitate the use of users, manufacturers usually configure an application software app. Through this app, users can access the monitoring video anytime and anywhere, which brings great convenience to people's lives. However, the corresponding software app of different cameras is different, and the same manufacturer uses more than one application software, which causes the uneven quality of camera mobile app in the market. And because the manufacturer does not pay attention to the security of this kind of application app, the vulnerabilities of these apps are more serious.

3. Camera System Security Protection Measures

3.1. For Consumers

For common users, due to the lack of expertise, the first thing we should do is to improve security awareness, understand how hackers attack the camera and understand how data is leaked. Secondly, when buying or configuring camera, it is necessary to buy through the proper channels,

choose a trusted supplier or a well-known brand. And be sure to keep in mind, do not covet little advantages. When choosing a camera, buy a device with basic protective measures. Change the default password for your camera as soon as you install it. It is recommended that you change it to a strong multi-character password. If possible, connect the camera to a network that is restricted to authorized users only. For remote monitoring, avoid public WIFI and unsecured, unknown networks. Keep relevant software and hardware up to date to ensure that the latest security fixes have been applied. Finally, pay attention to check the alarm information of the camera, and if you find abnormalities, contact the manufacturer or technician in time to deal with the problem.

3.2. For Operation and Maintenance Management Personnel

For the security operation and maintenance personnel of large camera systems, the latest security standards should be adopted to ensure that all cameras meet the standards. Secondly, regularly check the patch information released, and patch in time. Enforce only strong passwords and specify a password policy. Block ips that make multiple failed logins attempts to prevent brute-force attacks. Real-time detection of abnormal logs or alarm information is carried out to do a good job in dealing with abnormal conditions. Finally, the security of the camera system was analyzed and evaluated regularly by using vulnerability scanning tools, and the security weaknesses were identified and the corresponding measures were taken to repair them.

3.3. For Manufacturers

For the manufacturers of production equipment, they should follow the safety development standards during the development, pay attention to both function and safety, and conduct comprehensive testing and audit of the products before they are put on the market, so as to find and repair possible security loopholes and defects. Firmware should be regularly updated to fix known vulnerabilities and strengthen security functions to ensure that the latest security fixes have been applied. Finally, provide security guidelines to advise users on best practices to help them better understand and use the camera.

3.4. For the Nation and Society

For the country, we should improve the relevant security laws, not only to restrict the invasion of their privacy security behavior but also to reduce the threat from the source, strengthen the safety production supervision of manufacturers, but also actively popularize the camera security awareness, so that people develop the habit of regulating the use of cameras.

4. Conclusion

Camera has now become the choice of many people; camera system security is also an important component of network security. Improving the security of the camera system needs to unite the forces of all parties, and improving the security of the camera system is imminent. In the near future, the camera system will be a safe and reliable tool.

References

[1] Li Xiaojie An automated protection system for camera network security [J] Fujian Computer, 2022, 38 (10): 92-94. DOI: 10. 16707/ j.cnki.fjpc.20222.10.022.

[2] Xia Lingling, Zhang Zhenhao, Zhuge Chengchen, et al The Security Risks and Countermeasures of IoT Cameras in the Internet [J] Information Recording Materials, 2021,22 (3): 191-193.

[3] Bao Min Analysis of Network Security Issues and Countermeasures for Home Intelligent Cameras [J] Modern Information Technology, 2019, 3 (13): 172-174 DOI: 10.3969/ j. issn. 2096-4706.2019.13.069.

[4] Li Juan, Yu Zhongchen, Han Wenying Security Risk Analysis of IoT Cameras in Smart Cities [J] Information Security and Communication Confidentiality, 2017 (12): 40-48 DOI: 10. 3969/ j.issn.1009-8054.2017.12.008.

[5] Lu Weirao, Zhao Min, Golden Pigeon, etc Overview and automation of vulnerability detection methods for IoT surveillance cameras [J] Network Security Technology and Applications, 2019 (7): 91-92 DOI:10.3969/j.issn.1009-6833. 2019. 07.054.