Dahua Webcam Sensitive Information Disclosure Vulnerability Analysis

The Knownsec 404 Team

2017-03-21

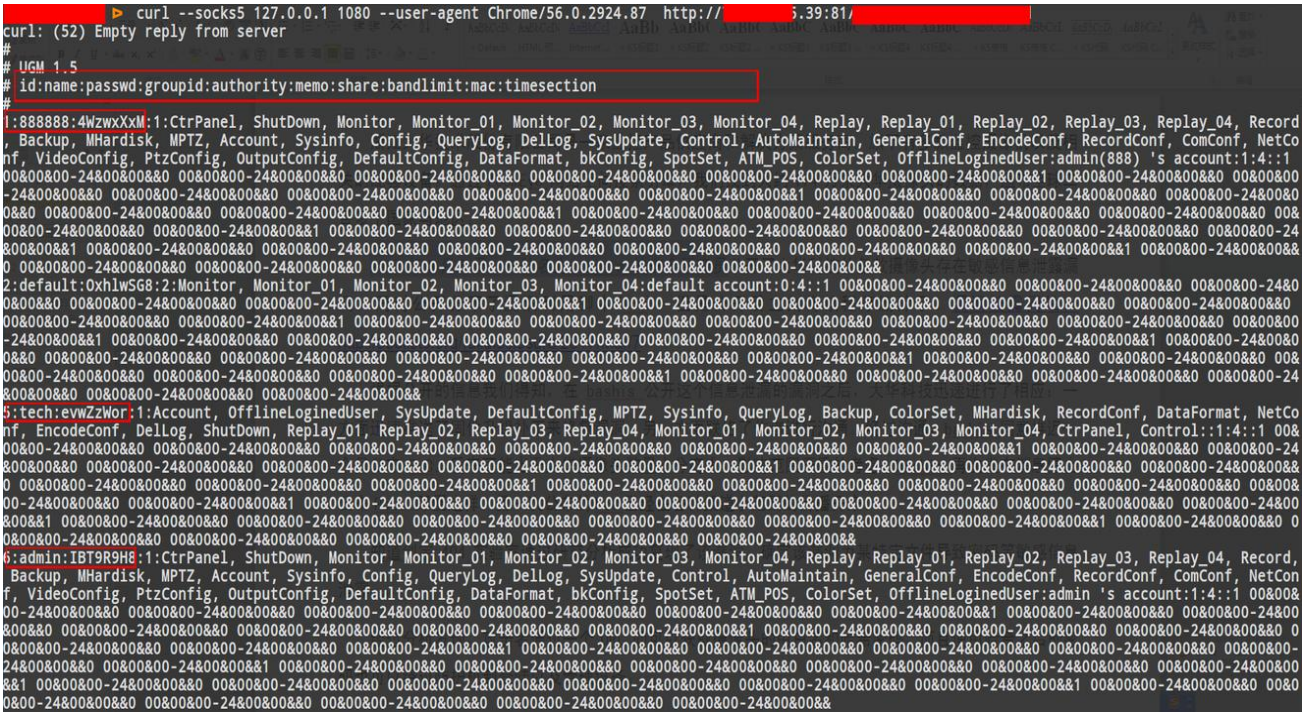
1. Update Status

Version	Time	Description
V0.1	2017/03/19	Basic Module Completed
V0.2	2017/03/20	Incident Timeline Description in Overview Completed
V0.3	2017/03/21	Global Distribution Statistics of iMaxCamPro Vulnerable Devices Completed
V1.0	2017/03/21	Official Release After the Review Process

2. Overview

Zhejiang Dahua Technology Co., Ltd. (Dahua) is a leading product and solution provider in the global video surveillance industry. They had the 2nd highest market share of global video surveillance equipment market in 2015 according to IHS 2016 report and ranked 4th in 2016 by a&s Security 50, which ranks global security industry players according to total security equipment sales. On March 5th 2017, the vulnerability platform seebug.org under Knownsec [0] recorded the vulnerability announcement by a foreign security researcher “bashis” who claimed that multiple Dahua Webcams have the vulnerability [1]. On the very next day, Dahua confirmed the vulnerability officially in Security-Bulletin_030617 and repaired it in its latest firmware [2].

The Knownsec 404 Team reproduced the vulnerability and confirmed its type as sensitive information disclosure after the analytical research, proving that attackers can obtain leaked information such as username and hashed password by accessing a link without any credential：



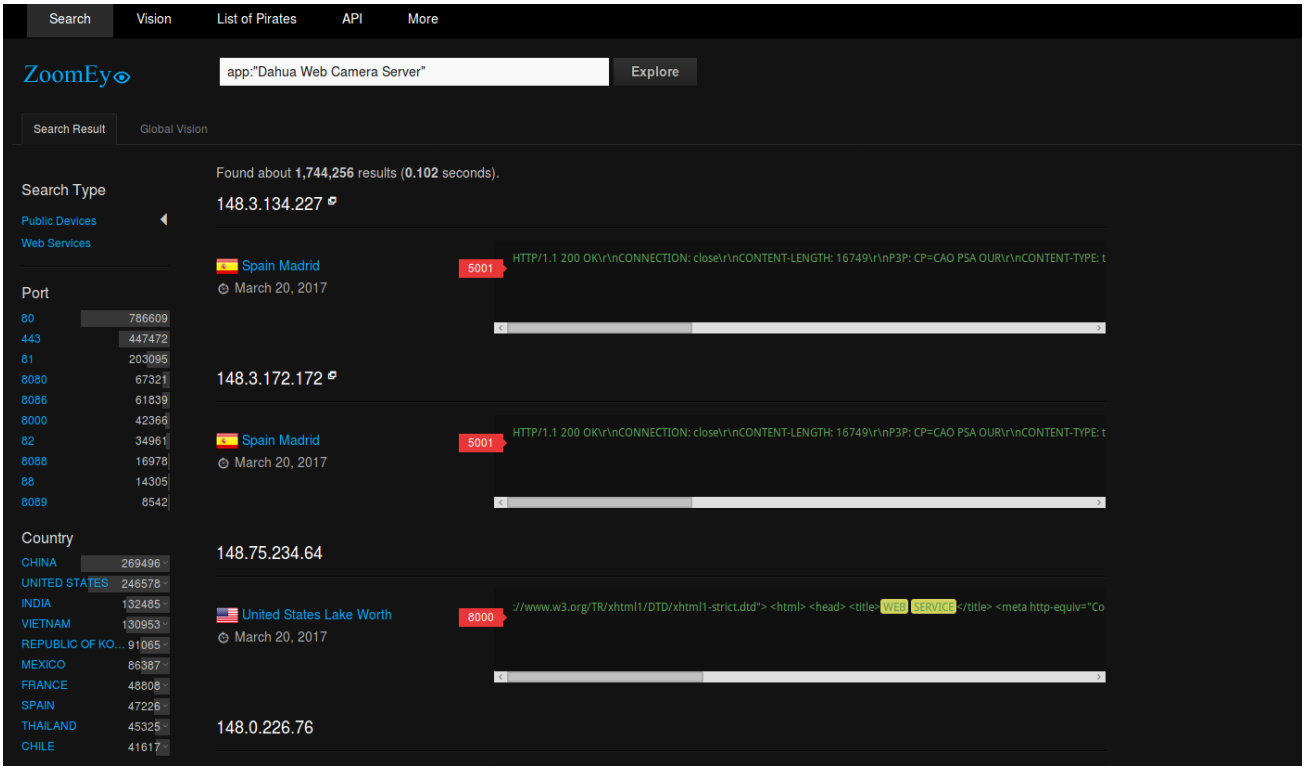
Attackers can manipulate the Webcam via the above leaked username and hashed password. Soon after, the Knownsec 404 Team detected the cyberspace using the ZoomEye search engine on March 19th 2017 [3]. The result shows that more than 200,000 Webcams on the Internet still had such vulnerability and this might also influence Webcam devices of other brands.

3. Influence Scope

2.1 The Total Amount of Vulnerable Devices

Using the default Dork (searching conditions) provided by ZoomEye, we can find the IP addresses related to 1,744,000 Dahua Webcams[4].

https://www.zoomeye.org/search?t=host&q=app%3A%22Dahua+Web+Camera+Server%22

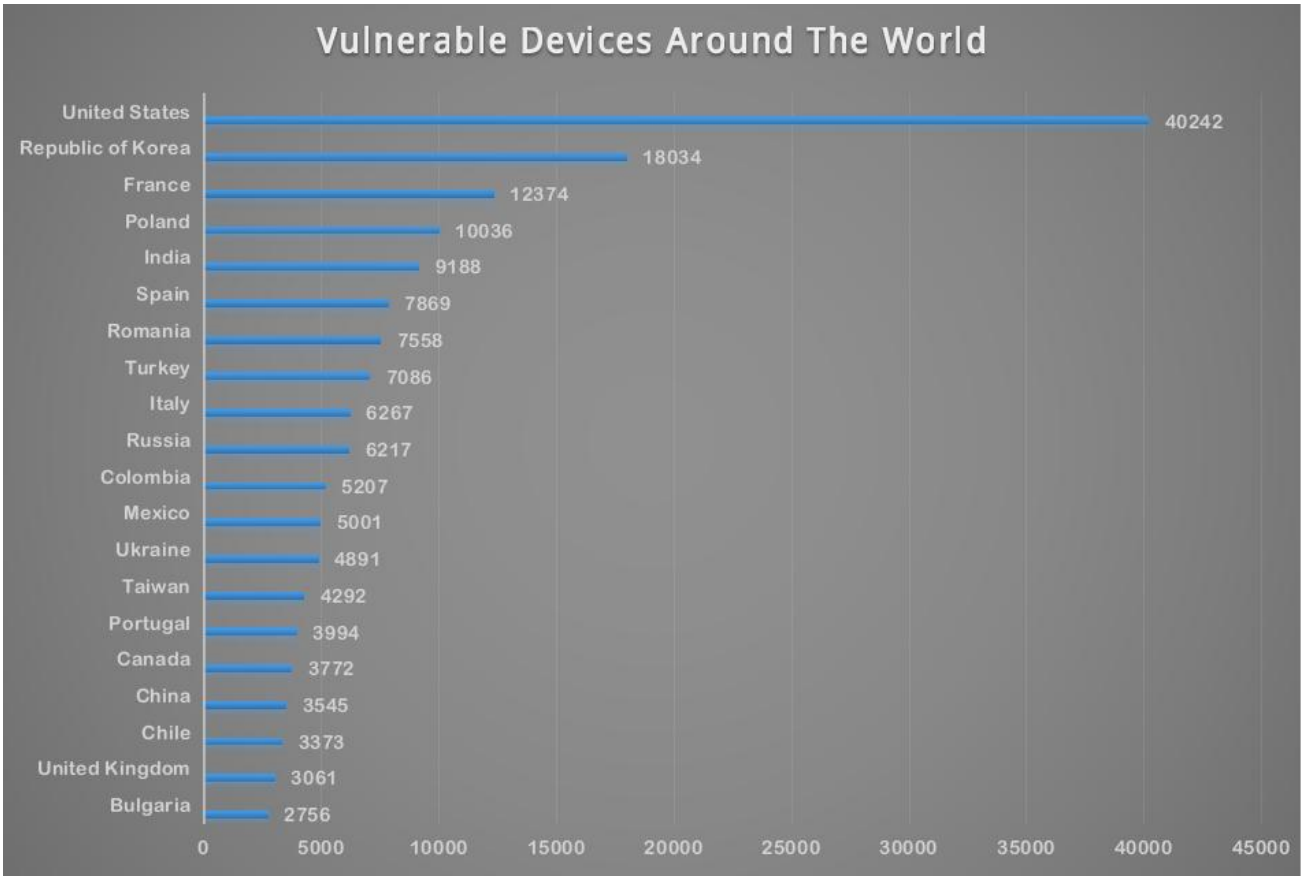


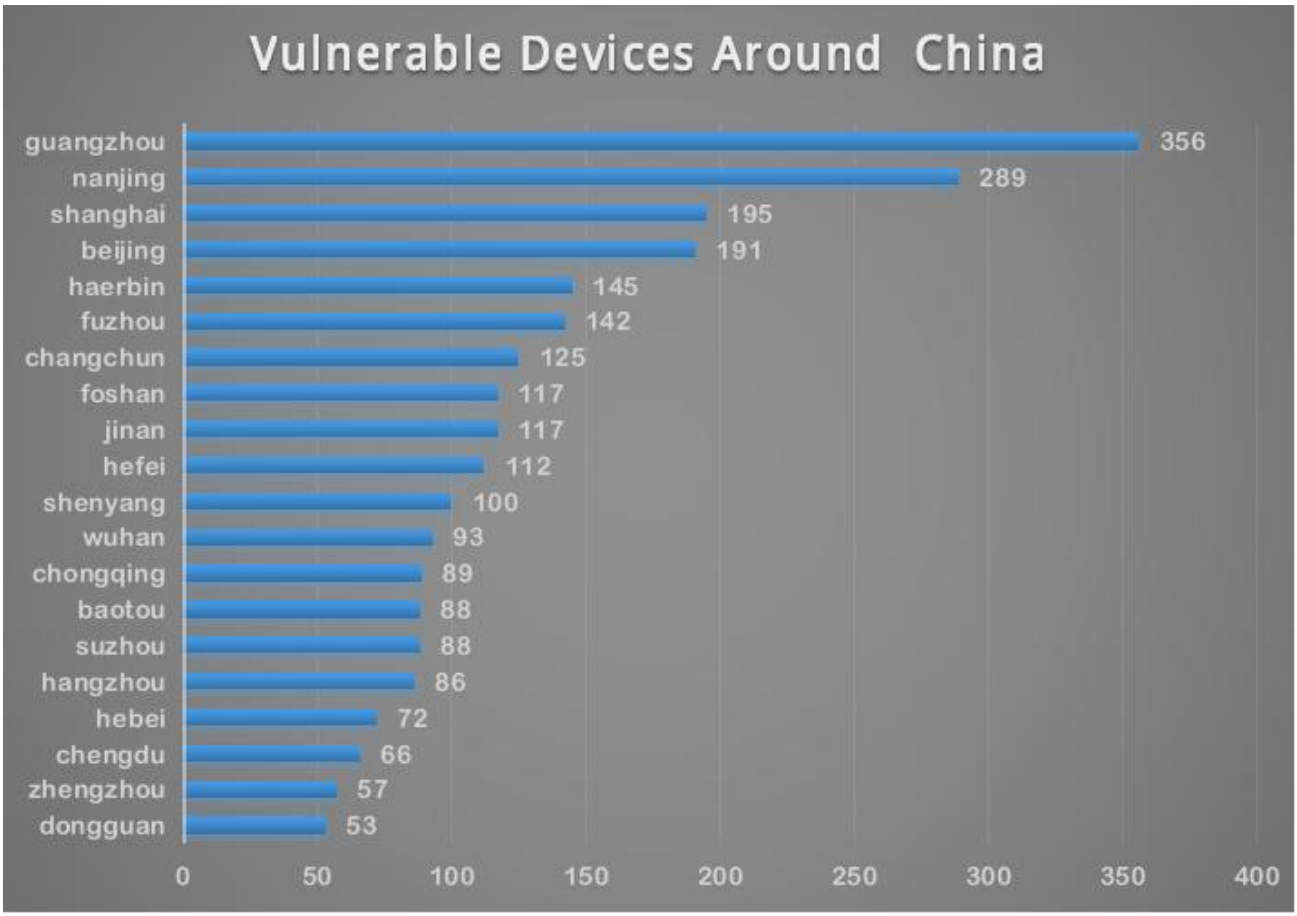
2.2 The Amount of Risk Devices Influenced by This Vulnerability

According to the ZoomEye detection result on March 19th 2017, there were still 206,000 devices having such vulnerability until 13 days after Dahua released the upgrade notice officially. The above is the statistics and analysis aiming at the risk devices.

2.2.1 The Geographical Distribution of Risk Devices

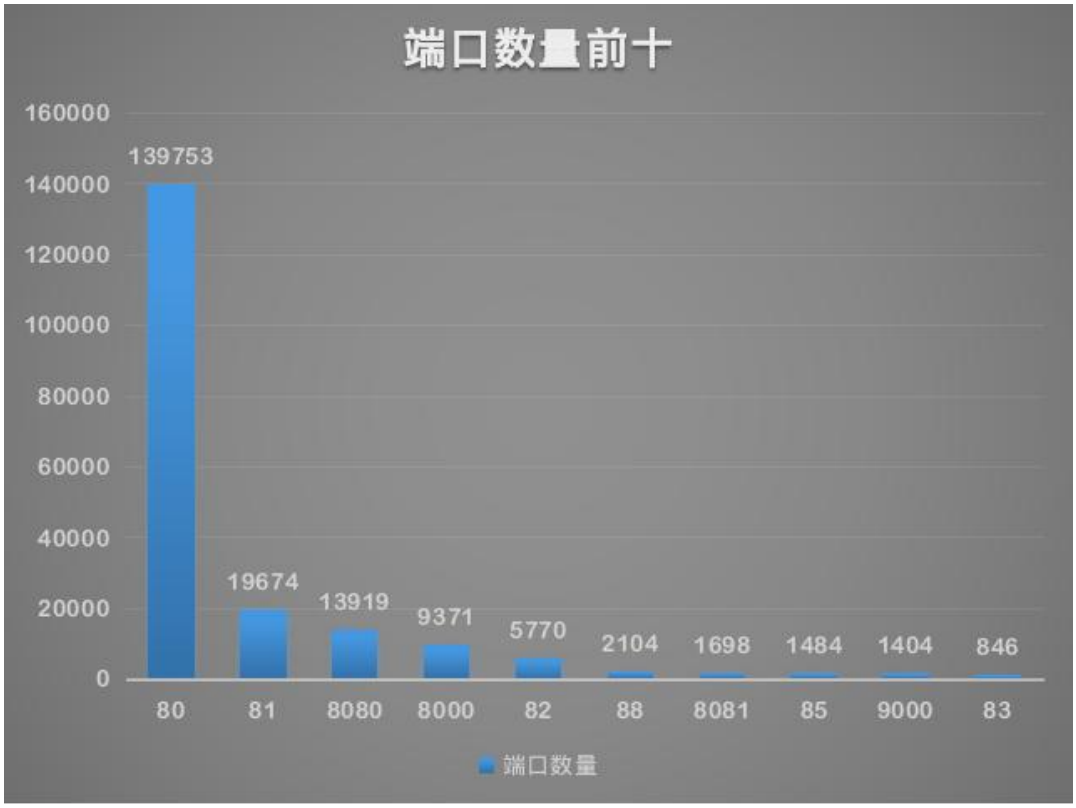
From the figure below, we can see that risk devices are distributed within 178 countries across the world. Among them, the USA and the European, African and South Asian countries have the most risk devices. In China, cities including Beijing, Shanghai, Guangzhou, Nanjing, and Harbin have the most risk devices.


Vulnerable Devices Around The World
United States 40242
Republic of Korea 18034
France 12374
Poland 10036
India 9188
Spain 7869
Romania 7558
Turkey 7086
Italy 6267
Russia 6217
Colombia 5207
Mexico 5001
Ukraine 4891
Taiwan 4292
Portugal 3994
Canada 3772
China 3545
Chile 3373
United Kingdom 3061
Bulgaria 2756
0 5000 10000 15000 20000 25000 30000 35000 40000 45000


Vulnerable Devices Around China
guangzhou 356
nanjing 289
shanghai 195
beijing 191
haerbin 145
fuzhou 142
changchun 125
foshan 117
jinan 117
hefei 112
shenyang 100
wuhan 93
chongqing 89
baotou 88
suzhou 88
hangzhou 86
hebei 72
chengdu 66
zhengzhou 57
dongguan 53
0 50 100 150 200 250 300 350 400

2.2.2 The Port Distribution of Risk Devices

In the real detection, we found that the Web services of risk Webcams were distributed in different ports. Besides, there were also other related open ports. According to statistics, there were 248 open ports on the Internet. The figure below shows the top ten open ports. It can be seen that most services are accessible on port 80. But it also happened that many installers and operators moved the services into other ports. Such behaviors can enhance the security of devices.



2.2.3 The Brand Distribution of Risk Devices

To further analyze the vulnerable devices, we extracted the MD5 checksum of favicon.ico on these devices' servers. A total of five MD5 values and the corresponding numbers were found:

bd9e17c46bbbc18af2a2bd718dddad0e	197634
b39f249362a2e4ab62be4ddbc9125f53	5885
bd1b5fef10a0846b2db322b90a57b746	109
d1ef1b4b9ef37b9dabec2db9e338de0f	237
a9d07db4284b4bdb144831a9ebb8dfd7	1546

Note that the other 496 devices did not have the favicon.ico file.

We chose partial targets in five groups of MD5 values to perform real access, webpage code analysis and discovery. The webpage coding of these five groups of MD5 values were similar in general. The "Dahua3.0-Web3.0" strings existed in related JavaScript codes. The major difference was the picture on the login page, shown as follow:

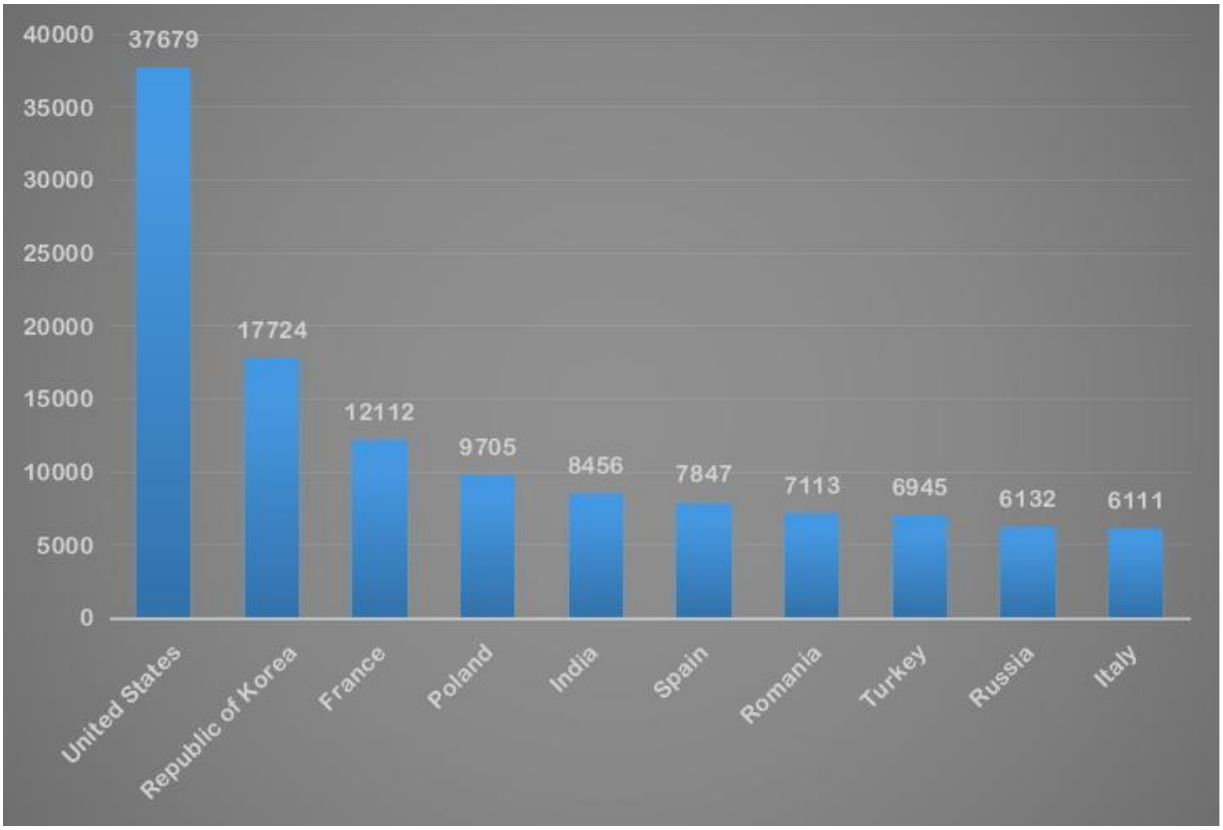
We noticed that the number of brand Webcams belonged to the "bd9e17c46bbbc18af2a2bd718dddad0e" group reached to 197,634, far exceeding those of the other four groups. The login page screenshot of these devices is shown as follow:

As no specific "brand" prompt was seen, we found the following webpage via Google Search [5]: https://www.worldeyecam.com/blog/technical-questions/configuring-ntp-imaxcampro.html and related to a brand Webcam named "iMaxCamPro".

According to the above analysis, we boldly speculated that the MD5 values from the five groups of favicon.ico files belonged to Webcam devices of different brands are based on Dahua devices. The specific release is shown as follows [6][7][8][9][10]:

title	产品名	数量	MD5	相关link
WEB SERVICE	iMaxCamPro	197634	bd9e17c46bbbc18af2a2bd718dddad0e	https://www.worldeyecam.com/blog/technical-questions/configuring-ntp-imaxcampro.html
WEB 1.0	CRECREDIT TECHNOLOGY	5885	b39f249362a2e4ab62be4ddbc9125f53	http://crecreditcctv.com/
dahua	大华摄像头	109	bd1b5fef10a0846b2db322b90a57b746	http://www.dahuatech.com/
HI-FOCUS	HI-FOCUS	237	d1ef1b4b9ef37b9dabec2db9e338de0f	http://hifocuscctv.com/
Honeywell	Honeywell	1546	a9d07db4284b4bdb144831a9ebb8dfd7	https://www.honeywell.com/
无	无	496	无	无

We continued global distribution add-up to most ranked brand Webcam probably named “imaxcampro”:



It can be seen that these devices are mainly located in oversea markets including America, Europe as well as Korea and India in Asia.

4. Detection & Fix

Detection:

Due to the large impacts, releasing detection tools might cause the disclosure of the vulnerability details. The researcher who found the vulnerability deleted the related PoCs on the same day after the vulnerability bulletin was released. Considering these factors, related detection codes are omitted here. For the organizations who need to check the security of their devices, please contact the Knownsec 404 Team.

Fix:

Dahua confirmed the vulnerability officially in Security-Bulletin_030617 on March 6th 2017 (http://us.dahuasecurity.com/en/us/Security-Bulletin_030617.php) by stating the affected device types and the upgrade method. Refer to [2] for more details.

For the other affected brands, the Knownsec 404 Team is actively getting in touch with related vendors to help them confirm and fix these vulnerabilities.

5. Conclusion

During this incident, Dahua carried out the emergency response process immediately after the vulnerability was disclosed. The vulnerability was confirmed and the related bulletin and firmware upgrade was finished. From the global statistics and brand analysis, it can be seen that only 109 risk devices are marked as Dahua. This shows that the emergency response by Dahua works great, which also implies that devices of different brands based on the same product still have large influence. This case also reflects the security status of the IoT industry. Generally, the cooperation between different venders still lacks the corresponding security procedure so far, which has already become a critical flaw for IoT devices.

6. References

[0]. Seebug Vulnerability Platform, https://www.seebug.org/

[1]. 0-Day: Dahua Backdoor Generations 2 and 3, https://www.seebug.org/vuldb/ssvid-92745

[2]. Dahua Security Bulletin March 6th 2017,

http://us.dahuasecurity.com/en/us/Security-Bulletin_030617.php

[3]. ZoomEye Cyberspace Search Engine, https://www.zoomeye.org/

[4]. Searching for Dahua Related Webcams with ZoomEye Cyberspace Search Engine,
https://www.zoomeye.org/search?t=host&q=app%3A”Dahua+Web+Camera+Server"

[5]. Configuring Automatic Time Updating for iMaxCamPro DVRs and NVRs,
https://www.worldeyecam.com/blog/technical-questions/configuring-ntp-imaxcampro.html

[6]. CRECREDIT TECH, http://crecreditcctv.com/

[7]. Dahua Tech, http://www.dahuatech.com/

[8]. Hi-Focus, http://hifocuscctv.com/

[9]. Honeywell International Inc., https://www.honeywell.com/

[10]. Worldeyecam, INC, https://www.worldeyecam.com/about-us.html