大华摄像头敏感信息泄露漏洞事件分析

知道创宇 404 实验室

2017-03-21

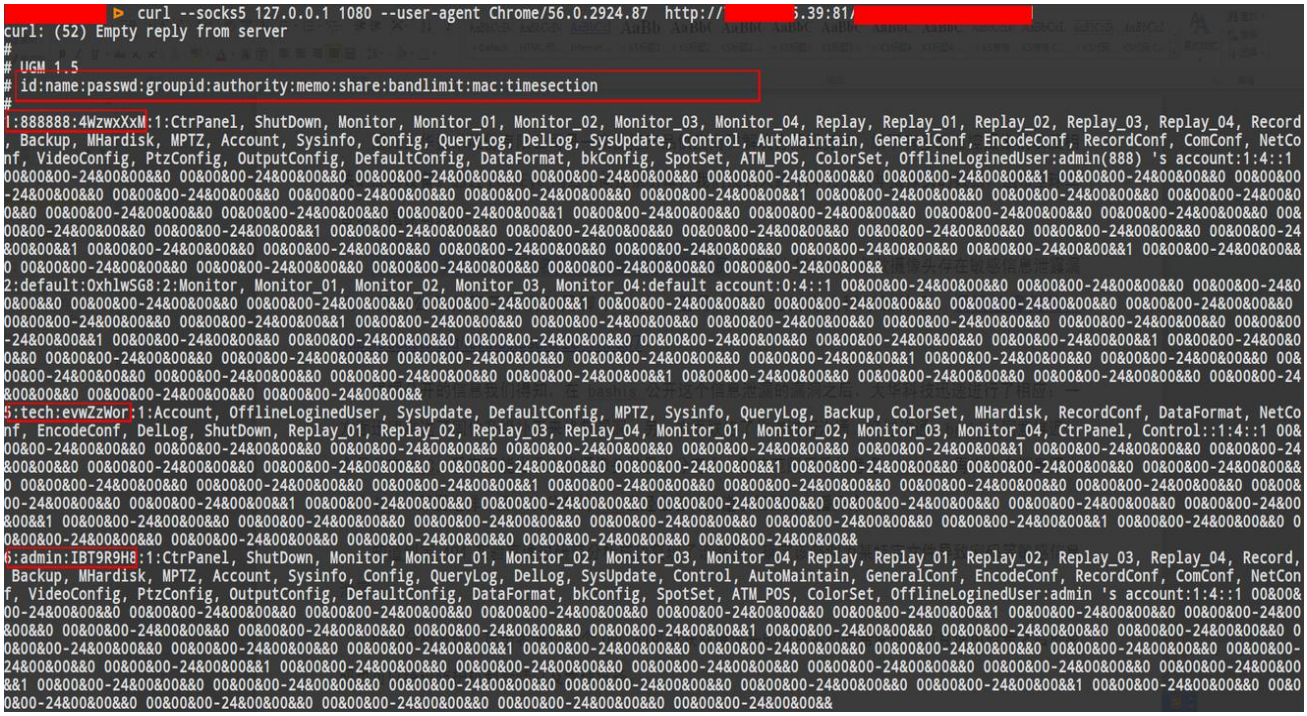
1. 更新情况

版本	时间	描述
V0.1	2017/03/19	完成大华摄像头敏感信息泄露数据分析报告基础模块
V0.2	2017/03/20	完善概述部分中关于事件时间线的描述
V0.3	2017/03/21	追加关于 iMaxCamPro 风险设备在全球分布统计信息
V1.0	2017/03/21	通过审核后正式发布报告《大华等品牌摄像头敏感信息泄露事件分析》

2. 事件概述

浙江大华技术股份有限公司是一家监控产品供应商和解决方案服务商。旗下有多款监控摄像机以及相关的配套设备。2017 年 3 月 5 日，知道创宇旗下漏洞平台 Seebug[0]上收录了一位名为“bashis”的国外安全研究员发布了一个漏洞公告，声称大华科技的多款摄像头存在“backdoor”漏洞[1]。随即在 2017 年 3 月 6 日大华官方在发布漏洞公告称(Security-Bulletin_030617)里确认了该漏洞存在并发布了最新的固件里修复了该漏洞[2]。

知道创宇 404 实验室通过研究分析成功复现了该漏洞，确定该漏洞是一个敏感信息泄露漏洞。攻击者无需任何凭证的情况下访问一个链接即可得到摄像头设备 Web 管理的用户名和哈希密码等信息泄露：



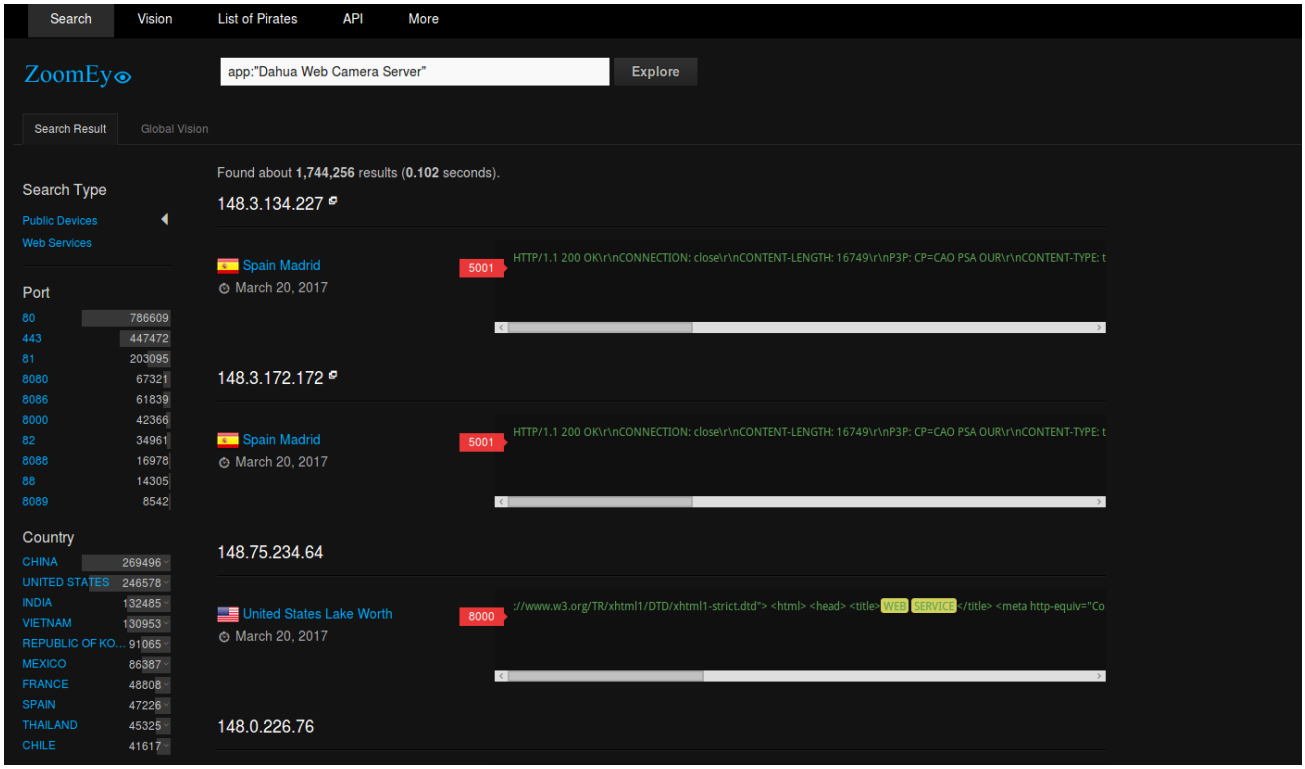
攻击者通过这个泄露的用户名和哈希密码可直接控制管理该摄像头设备。随后知道创宇 404 实验室通过“ZoomEye 网络空间搜索引擎”[3]并于 3 月 19 日对全网进行探测。3 月 19 日的数据结果显示互联网上仍然有 20 多万的摄像头设备存在该漏洞，并可能影响到除大华品牌外的其他多个品牌摄像头设备。

3. 漏洞影响范围

2.1 设备总量

我们使用 ZoomEye 提供的默认 Dork(搜索条件)，可以发现 ZoomEye 网络空间搜索引擎历史上收集了 174.4 万大华摄像头相关的 IP 数据[4]。

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

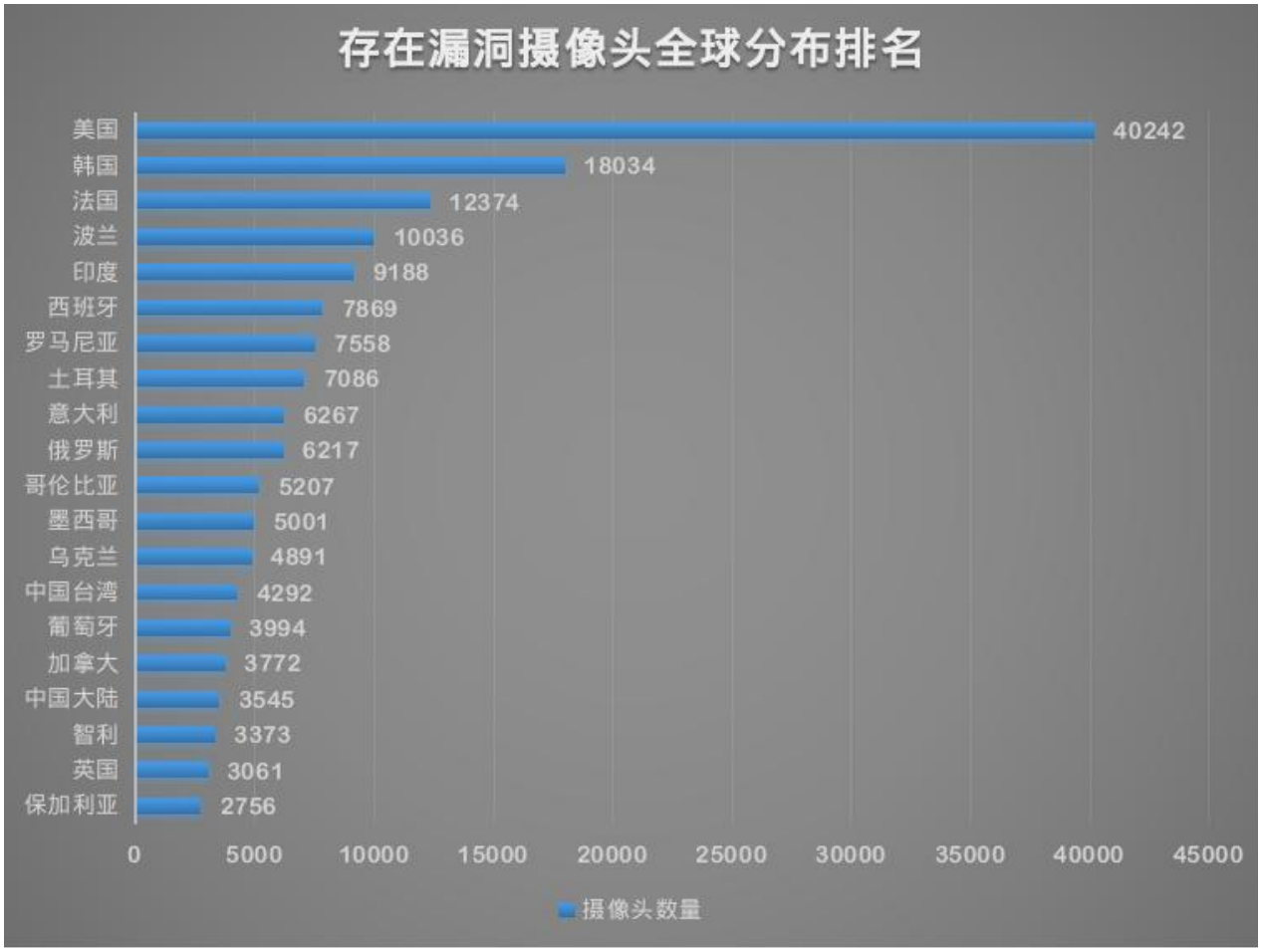


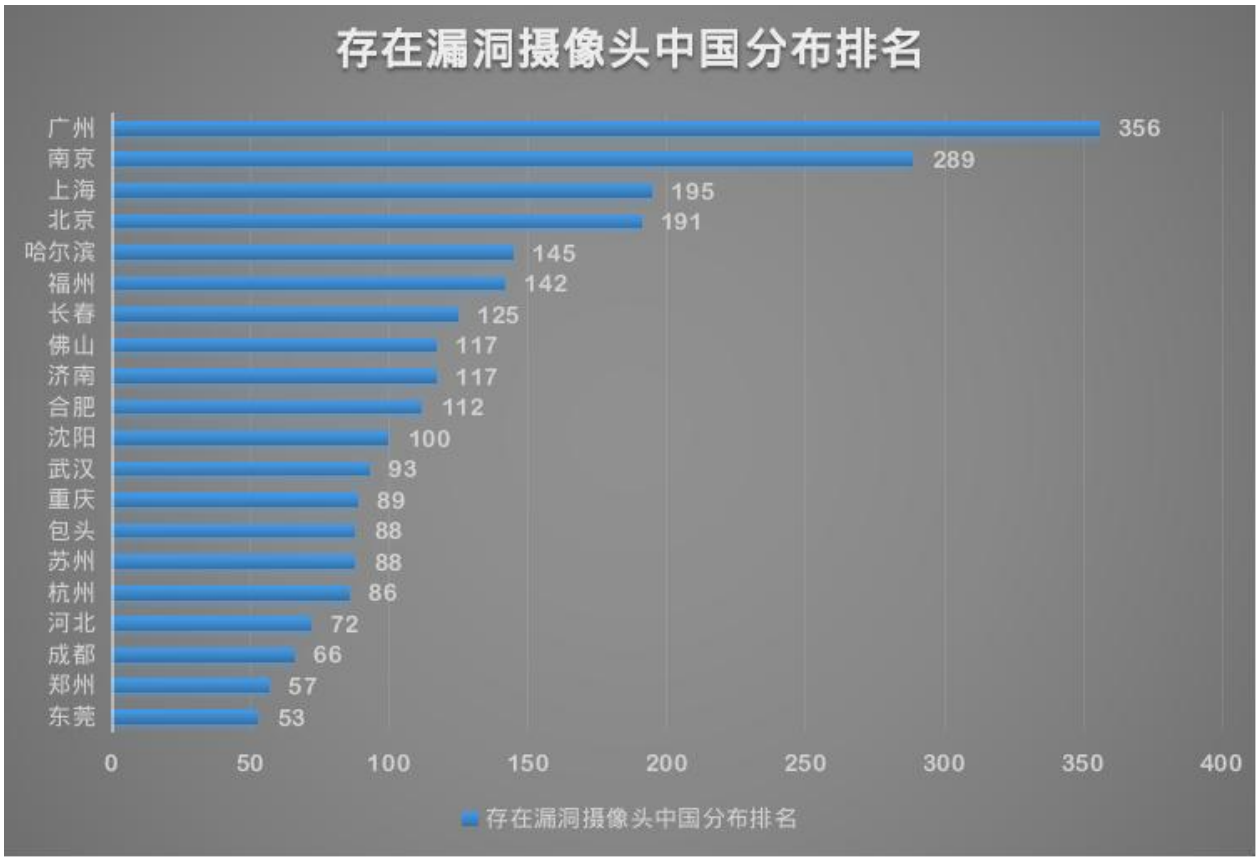
2.2 受漏洞影响的风险设备的数量

针对知道创宇 404 安全实验室于 3 月 19 日通过对 ZoomEye 网络空间引擎对全球进行探测结果显示距离大华官方于 3 月 6 日发布升级公告后（13 天）全球仍然有 20.6 万设备存在该信息泄露漏洞。以下是针对风险设备的统计和分析。

2.2.1 风险设备的地区分布

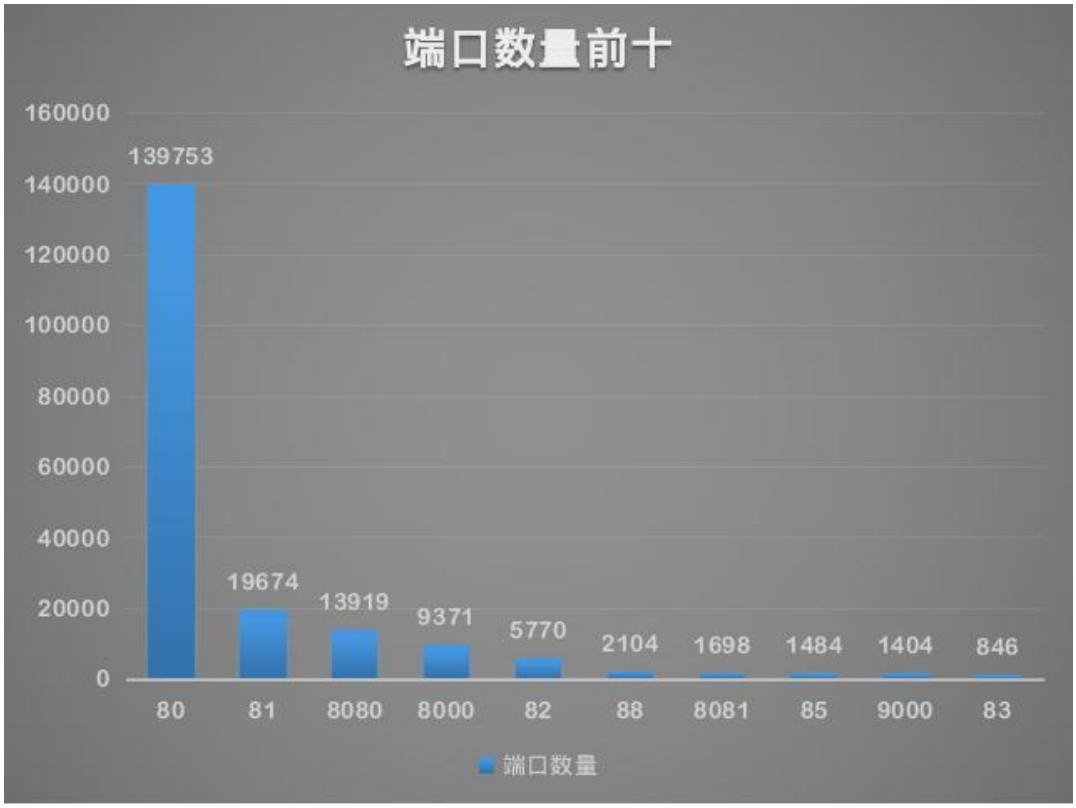
由下图可见，风险设备分布在全球 178 个国家中。在全世界范围内，美国、欧洲、非洲以及南亚地区的风险设备数量较多。而中国区域内，北京、上海、广州、南京和哈尔滨这几个城市风险设备最多。


存在漏洞摄像头全球分布排名
美国 40242
韩国 18034
法国 12374
波兰 10036
印度 9188
西班牙 7869
罗马尼亚 7558
土耳其 7086
意大利 6267
俄罗斯 6217
哥伦比亚 5207
墨西哥 5001
乌克兰 4891
中国台湾 4292
葡萄牙 3994
加拿大 3772
中国大陆 3545
智利 3373
英国 3061
保加利亚 2756
0 5000 10000 15000 20000 25000 30000 35000 40000 45000
摄像头数量


存在漏洞摄像头中国分布排名
广州 356
南京 289
上海 195
北京 191
哈尔滨 145
福州 142
长春 125
佛山 117
济南 117
合肥 112
沈阳 100
武汉 93
重庆 89
包头 88
苏州 88
杭州 86
河北 72
成都 66
郑州 57
东莞 53
0 50 100 150 200 250 300 350 400
存在漏洞摄像头中国分布排名

2.2.2 风险设备的端口分布

在实际的探测中，我们发现风险摄像头的 Web 服务开在了不同的端口，除此以外还有各种其他的端口开放。根据统计，共有 248 个端口开放在互联网上，下图是数量最多的十个端口。由下图可见，大多数服务还是开放在 80 端口，但是也有很多安装、运维人员将端口修改到了其他端口，这样的行为在一定程度上是能够增加设备的安全性的。



2.2.3 风险设备的品牌分布

针对这些存在漏洞的设备尝试进行进一步分析，我们提取了这些设备服务器上的 favicon.ico 的 MD5 值校验，总共发现了以下五组 MD5 值及对应数量：

bd9e17c46bbbc18af2a2bd718dddad0e	197634
b39f249362a2e4ab62be4ddbc9125f53	5885
bd1b5fef10a0846b2db322b90a57b746	109
d1ef1b4b9ef37b9dabec2db9e338de0f	237
a9d07db4284b4bdb144831a9ebb8dfd7	1546

注：另有 496 个设备不存在 favicon.ico 文件

我们分别选取了 5 组 md5 里的部分目标进行实际访问及网页代码分析发现，这五组 md5 的网页代码都基本相似，在相关的 JavaScript 脚本代码里都存在“Dahua3.0-Web3.0”字符串，主要的区别是在 WEB 管理登录页面图片不一样。如：

我们注意到“bd9e17c46bbbc18af2a2bd718dddad0e”组的品牌摄像头数据量多达 197634，远远超过了其他 4 组的数据，这些设备的登录页面截图如下：

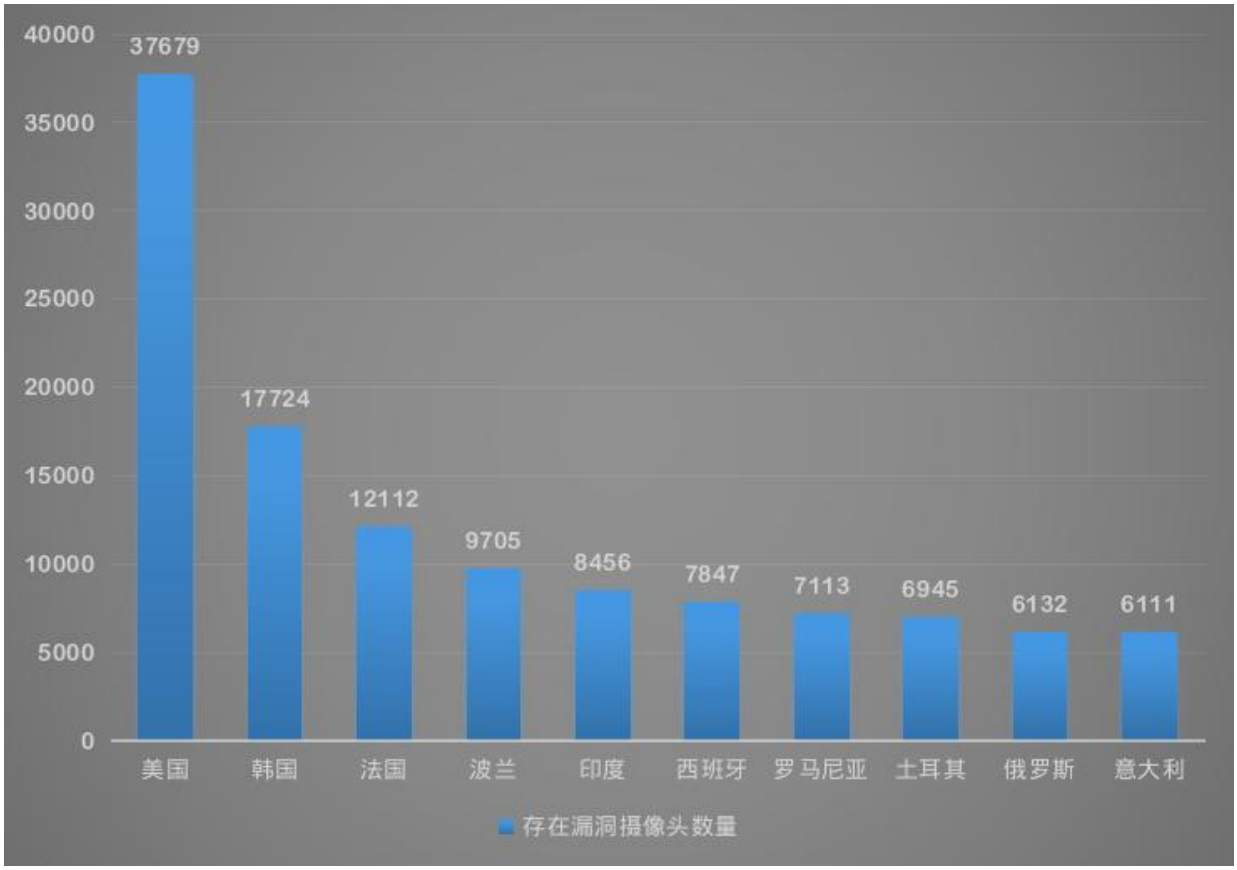
没有看到明确的“品牌”提示，于是我们通过谷歌得搜索找到如下网页[5]：

https://www.worldeyecam.com/blog/technical-questions/configuring-ntp-imaxcampro.html 关联到一个叫“imaxcampro”的品牌摄像头。

根据以上分析，我们大胆的推测 5 组不同的 favicon.ico 文件 md5-hash 的品牌的摄像头设备基于大华设备修改而来，具体发布如下[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

针对排名最多的疑似叫“imaxcampro”的品牌摄像头继续进行了全球地区分布统计：



可以看出这些设备主要分布在美欧及亚洲的韩国印度等海外市场。

4. 检测与修复

检查方法：

由于该漏洞影响较大发布检测工具可能导致漏洞细节的泄露，另漏洞发现者在漏洞公告当天就删除了相关漏洞验证程序，所以这里暂时不提供相关检测程序。对于使用上述品牌摄像头需要检查相关设备安全的单位或组织，请与知道创宇 404 实验室联系。

修复方法：

针对该漏洞大华官方在 3 月 6 日就发布了相关的漏洞公告、影响设备型号及升级方法 详见[2]：

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

针对其他影响的品牌目前知道创宇 404 实验室正在积极联系相关厂商确认并协助修复相关漏洞。

5. 结论

在此次事件根据及分析过程中该漏洞被披露后大华公司随即进行了安全应急响应确认了漏洞并发布了相关公告及固件升级，从 13 天后的全球统计数据及品牌分析标注了 dahua 的品牌只占有 109 个，从这个角度来看说明大华公司的应急是有显著的效果的，同时也说明基于同一种产品不同品牌的设备影响还非常大。这个案例也反映了一个存在于 IoT 等设备安全现状：厂商或品牌的合作流程里目前广泛缺少了对应的“安全”流程，这显然已经成为 IoT 设备安全一个重要的“缺陷”。

6. 参考链接

[0]. Seebug 漏洞平台 https://www.seebug.org/

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

[2]. Dahua Security Bulletin March 6, 2017

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

[3]. ZoomEye 网络空间搜索引擎 https://www.zoomeye.org/

[4]. ZoomEye 网络空间搜索引擎搜索大华相关摄像头设备

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