网络空间测绘系列
2018年摄像头安全报告

北京华顺信安科技有限公司

前言

随着中国网络安全的发展，网络安全逐渐受到国家重视。习主席也提出“没有网络安全，就没有国家安全”。而其中国家最重视的则是关键信息基础设施。在 2017 年正式施行的《网络安全法》中，明确提出关键信息基础设施的安全法则。因此对关键信息基础设施的检测至关重要，其中检测的技术主要是网络空间测绘技术。网络空间测绘技术是 2016 年新提出的概念，网络空间测绘是通过对全球网络对外开放服务的资产进行主动或被动方式探测、抓取、存储，分析整理不同种类的网络空间资产指纹信息（规则），并对符合规则的资产进行统计分析，进而快速检索全球网络空间资产。它能够帮助用户迅速进行网络资产匹配，快速开展网络空间威胁态势感知、漏洞影响范围分析、应用分布统计、应用流行度排名统计等工作，并对关键信息基础设施进行良好管理。白帽汇安全研究院计划利用网络空间测绘技术开展系列性主题报告。该报告则主要是基于网络空间测绘技术进行网络摄像头的安全分析。

随着“互联网 +”模式的兴起，物联网（IoT，Internet of Things）呈现出爆发式增长和普遍化发展的趋势。物联网技术的不断革新，已经深深地影响并改变着人们的生活。大量与之相关的应用型新产品、新服务和新模式也应运而生，并形成了一套完整的物联网生态系统。至此，物联网技术成为催生产业、经济和社会发展新浪潮的重要力量。

如果说在互联网时代，硬件和系统漏洞带来的危害尚局限于用户

信息安全泄漏，那么在万物互联时代，由其衍生的危害将拓展至我们的人身安全生态。未来，越来越多的“物”（包括手机、PC 和平板电脑等家庭智能电子设备和智能摄像头、城市联网汽车和智能路灯、工厂智能生产设备等）将被连接到网络。这些设备一旦被居心不良者远程控制并进行恶意操作，无疑将对个人和家庭带来超乎想象的危害。而这些危害的形成，一方面是源于设备数量众多，安全性被使用者忽视。廉价的摄像头、监视器等物联网应用产品大量出现，但这些产品往往没有采取任何安全措施，黑客能够轻易地控制它们；另一方面，随着物联网设备的增多，硬件难以更新。未来几年，僵尸网络的规模会越来越大，攻击能力越来越强。

以摄像头为例，物联网中摄像头的应用已经遍及城市交通、企业内部、医院、银行、家庭等生产生活的各个场景。随着摄像头使用量的不断增加和应用场景的不断拓展，摄像头安全之于社会生活、生产的重要性日趋显著。然而，随摄像头应用拓展而来的则是一条集黑客破解、买卖、偷窥于一体的视频摄像头网络黑产链。

基于此背景，如何在正确认识这一黑产业链运作构架的基础上，提出促进摄像头安全及其生态系统健康发展的破解之法，是摄像头等智能设备在物联网时代实现安全发展的重要突破点。白帽汇安全研究院利用网络空间测绘技术，以“摄像头安全现状报告”的形式，从暴露情况、漏洞、隐患等多方面对摄像头应用现存的安全威胁和相关黑色产业攻击行为进行深度剖析，并可以利用网络空间测绘技术对摄像头进行安全排查，搭建安全防护体系，从根源上促使摄像头使用生态

实现优化，继而希冀为我国摄像头产业的安全健康发展提供有利的助益。

本报告在编写过程中参考大量资料，对资料的作者和提供者深表感谢。

Revision Record 修订记录

Date 日期	Revision Version 修订 版本	CR ID / Defect ID CR号	Sec No. 修改 章节	Change Description 修改描述	Author 作者

Distribution List 分发记录

Copy No.	Holder's Name & Role 持有者和角色	Issue Date 分发日期
1		
2		
3		
4		
5		

目录

1 摄像头安全概述

1.1 背景

随着生活“智能化”程度的不断加深，手机、监控、视频等摄像头设备已融入到生活的各个方面。人们利用摄像头进行视频聊天、监控宠物、安全防护等。然而，这些摄像头具备的联网和云端存储，甚至公网开放服务等功能，在为人们提供便利的同时，也让为利益或猎奇心理所驱使的黑客有了可乘之机。黑客通过网络和云端能够更加容易地获取到摄像头的信息文件。部分摄像头也因此成为黑客的攻击对象。

此外，值得注意的是，视频输出是基于通用通信协议的，而无需特定的摄像头客户端，与 HTTP 协议类似，网络摄像头的协议几乎是相同的。至此，黑客便可随意调取摄像头内容。另外，与国内和国外网站都可通过浏览器实现信息浏览一样，网络摄像头在生产标准上也相对一致。这就意味着，一旦一个视频账号体系有缺陷且被渗透，将造成这一类账号体系被渗透的可能性直线上升。这也是摄像头隐私频被曝出的主要原因。

近两年诸多摄像头严重漏洞曝出事件频发。海康威视在 18 年 4 月被发现其云服务器存在严重的访问控制缺陷：只要获取用户 ID 就可以访问登录任意用户的账号。任意人都可通过该漏洞实现同步查看实时用户监控摄像和回放录像、添加账户共享、修改重置用户密码、修改用户绑定邮箱等操作，影响范围甚广。6 月，Axis 摄像头被 ADOO 安全公司发现其设备的 7 个安全漏洞，攻击者可以利用这些漏洞以 root 权限执行任意命令。8 月，Swann 摄像头被发现存在访问控制缺陷，该漏洞可以将一个摄像头的视频流切换到另一个摄像头上，攻击者可以利用该漏洞访问任意摄像头。9 月，安全研究公司 Tenable 披露 NUUO 安防类网络摄像头中的“Peekaboo”漏洞，攻击者可以利用该漏洞查看监控录像或者更改画面和音频。该漏洞影响到了全球数十万台闭路电视、监控设备等。

近两年黑客还通过摄像头设备漏洞植入其僵尸程序并发起 DDOS。2016 年，美国东海岸断网事件就是一款 Mirai 的物联网设备的僵尸程序导致的。Mirai 的传播方式主要以摄像头设备的 Telnet 和 SSH 弱口令为为主。后来该病毒被不断

修改，增加诸多变种，传播方式也增加多种 Nday 漏洞传播。

除此之外，近两年加密货币的发展盛行，也为利用摄像头设备传播挖矿病毒培育了土壤。

1.2 摄像头安全现状

摄像头的使用场景众多，在生活中随处可见,譬如家庭和公共场所的监控等。因摄像头涉及诸多隐私信息，摄像头的安全性也就显得尤为重要。目前摄像头品牌众多,产品参差不齐,没有安全标准和安全规范,由此衍生出了诸多安全隐患。

1.2.1 规模广、影响范围大

首先，为了降低研发成本，大部分品牌的摄像头都选择使用同一套底层软硬件。也就是说，不同品牌的摄像头往往只是“换壳”出现。这一现象使得摄像头的某个部件一旦出现了问题，就会牵涉到多个品牌。

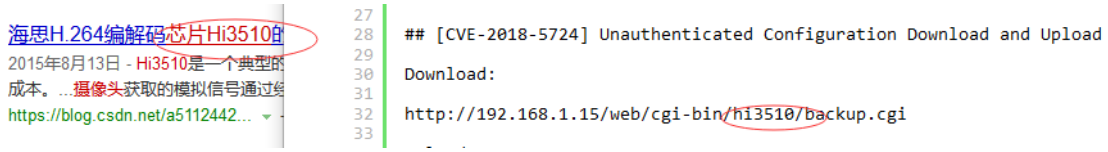

图 1-1 Hi3510 芯片广泛用于摄像头产品，一旦出现漏洞，影响极大

很多摄像头出于实现视频实时上传云端功能的考虑，往往为了追究较好的上传性能，使得出口带宽较大，从而带来三方面的问题隐患：

- 适合 DDos 攻击。黑客在完全控制摄像头的情况下迅速把带宽打满，而且市面上流行的摄像头芯片（如华为的海思芯片）性能较好，稳定性强，给予了黑客可乘之机；
- 加密与授权的问题。在摄像头与服务器交互以及上传视频到云上的过程中，很多厂商都没考虑加密与授权的问题，容易导致敏感信息泄漏以及中间人攻击的问题；
- 权限维持的问题。摄像头往往 24 小时在线，比桌面 Windows 更“稳定”，黑客无需考虑权限维持的问题。

其次，最经久不衰的漏洞——弱密码的出现。用户在安装摄像头时，由于没

有足够的安全意识，多数情况下不会对密码进行更改。同时，摄像头软件少有强制用户更改密码的设置。这直接导致黑客可以通过简单的密码字典，大范围爆破摄像头的管理密码。更可怕的是，各大品牌摄像头的默认密码均可以在网上找到。

图 1-2 曾经的 Mirai 物联网僵尸就是利用弱密码大范围攻击摄像头

1.2.2 摄像头安全管理体系不健全

根据高盛等市场研究公司日前发布的数据显示，截止到 2017 年，世界上的摄像头总数约为 14 万亿个，到 2022 年，全球摄像头总量将增至 44 万亿个。而对于手机来说，假设全球每人都使用两台，全球手机数目也不过为 150 亿台左右。这一数量等级的差距，决定了摄像头的监管和使用很难做到面面俱到，更不可能像手机一样做到一对一监管。大多数摄像头的监管，都是采用安排安保人员在监控室用转换屏幕的方式监控上百个摄像头。而这种监控方式造成的结果就是：一旦某个摄像头出现问题，既不能及时发现，也无足够的技术去修复。

此外，因往往处于某个（墙壁上）固定的位置，企业摄像头一旦出现资产方面的损坏、升级和换新等问题，企业将无法通过搬运统计的方式对其进行系统处理，从而使得企业在摄像头这一资产的整体控制方面存在管理空缺。

同时，在很多企业中，摄像头大部分都是处在内网环境中，很难借助远程网络服务来对摄像头进行检查盘点。值得说明的是，并不是处于内网的摄像头就是安全的，黑客只要接入内部网络，摄像头承载的信息将一览无余地暴露在攻击者的视野中。虽然很多公司都会对内部的网络划分出敏感区域和非敏感区域，控制客户网络访问 IP 权限，但是内部网络对很少摄像头进行单独划分，而这些存在漏洞的机器就很有可能成为黑客的后门。

1.2.3 更新不及时

大多数摄像头出于维持稳定性的考虑，通常是不会强制自动升级固件的。用户很难立即接收到自用摄像头存在的漏洞信息，也很少关注。用户只有在使用 APP 控制的时候，才有可能接收到更新信息。而此时，因很多更新提示并未对更新事项进行说明，用户往往会失去更新的动力，而选择跳过更新。更糟糕的是，大部分的摄像头目前并不是通过手机来管理，这就导致用户在购买摄像头之后，一直不知道摄像头有安全问题，更不会去进行更新。

在企业的场景中，与手机电脑类产品不同，出于稳定性的考虑，摄像头的安全更新机制很难做到完全强制更新（不更新就不能使用），而且通常没有远程更新机制。当手机和电脑出现严重漏洞威胁，厂商可立即推送补丁到设备上，并且可设定一定程度上的强制安全更新并给出较完善的安全提示。但摄像头则完全依赖用户的主动更新，如果某个品牌的摄像头的漏洞曝出，官方往往只能在官网提供一个更新的固件下载，暂无及时远程提示用户的有效手段。

而用户在摄像头能持续正常工作的情况下，也不会频繁关注安全补丁的更新，继而造成安全补丁的滞后，也为黑客的入侵提供了充足的操作空间。此外，当用户发现摄像头出现问题后，由于性价比等原因，多数用户并不会特意修理摄像头或安装补丁，而是将之直接弃置在家中，而这也变成了黑客利用的“温床”。

1.2.4 危害程度大

对普通用户来说，单个摄像头的安全与否似乎不会对日常生活产生严重的影响。但这些摄像头联合起来，就有可能造成巨大的威胁。2016 年 10 月，一场大规模互联网 DDos 攻击席卷了美国，包括亚马逊、ebay、推特等在内的多家知名网站无法正常登陆。安全研究人员表示，造成此次 DDos 事件正是由于以摄像头为首的大量物联网设备被黑客控制，并向关键的节点服务器发动 DDos 攻击，从而导致大量网站无法正常访问，而这些摄像头设备被指由中国的某大型摄像头厂商制造。

漏洞摄像头若被不当使用也将带来难以估计的安全威胁。据卡巴斯基报道，伦敦市内的摄像头与当地居民人口数比例达到了 1:10。这些摄像头几乎都采用

无线方式连接到互联网。虽然安装这些摄像头的初衷是打击犯罪活动，但是据安全人员调查，由于这些设备通常暴露在室外，很多网络犯罪分子能够轻易获取到摄像头的设备类型和名字，再根据网络上已曝出的相关漏洞或者逆向工程，轻松入侵设备，获取摄像头拍摄画面并远程操控提供虚假画面或直接让系统宕机，严重威胁着整个城市的安全。

相较于家庭网络监控摄像头，城市监控网络则更加复杂。由于数据传输需要经过多个中介点才能到达执法机构。一旦其中某个中介节点被黑客渗透控制，好莱坞电影里情节就将发生：黑客可以将虚假画面传至执法机构，既可造成某个地点发生重大安全事件的假象，又能确保在某地点真正存在的犯罪活动顺利进行。

1.2.5 安全防护难

物联网设备由于体积小，计算存储能力较计算机相差甚远。摄像头设备很难承载运行如计算机系统的防病毒或防火墙等防护应用。这一现状直接导致了因无需考虑反病毒等技术而受到黑客的喜爱。此外，目前也无相关厂商对这类安全防护技术展开大规模地研发、普及和大范围的应用，这无疑增加了用户进行安全防护的难度。

1.2.6 无防护手段

如今，智能摄像头已和手机一样，成为了能上网的“微型电脑”。但是，由于人们对这两类产品接触使用的时间不同，导致人们对两者的了解深度与使用要求也不同。例如，手机安全可以说是一直被反复提及的话题，厂商也都做出各种不同的努力来尽力提升手机安全性。从手机硬件上说，从以往的输入密码解锁，升级到画图解锁，演变出指纹解锁，再到现如今的 3D 人脸识别和虹膜识别，手机的安全性和便捷性得到了很大程度的提升。安全性，至此也成为手机新品发布会的重要内容，用户也愿意为之买账；就软件方面，各大手机厂商基本在自家品牌的手机上都安装有自主研发的安全管理 APP。与此同时，各种第三方的安全软件也层出不穷。这些安全软件不仅为手机提供各种安全防护和系统管理，还能为手机提供各种优化。而摄像头设备，唯一的验证方式就是通过密码登入，极少数才

有动态验证码，更别提人脸识别和安装防护软件之类的验证方式。

图 1-3 某个刚曝出漏洞的摄像头在淘宝依旧销量第一

图 1-4 众多网络摄像头价格只要几十元就可以买到

在摄像头安全还未被反复提及时，摄像头的安全性完全不是吸引顾客的要素之一。消费者大多追求产品的功能强大和强稳定性，而摄像头因漏洞被攻陷带来的不安全隐患完全不在考虑范围内。究其原因，主要是因为摄像头的使用历史不长，且不像手机那样为用户贴身携带。这就导致摄像头厂商对安全问题缺乏足够的重视，甚至在安全问题曝出之后，部分厂商想到的是如何掩盖问题，而不是修复问题。

1.3 摄像头安全风险

急速增长的摄像头数量和越来越多的摄像头漏洞预示着，在未来，摄像头安全将会成为继手机和电脑安全后的全球又一大重点安全领域。黑客通过攻击摄像头而造成的安全隐患影响的不仅是一个人或一群人，而是所有人。也就是说，即使不使用任何摄像头产品的人群，也将无法逃脱公共摄像头漏洞产生的危害影响。基于摄像头安全的发展趋势，近期，欧盟推出的《数据安全保护法》明确指出，企业如果对用户数据泄漏不作为将受到最高达 1500 万欧元的罚款。这一条款的出台无疑将促使大量企业提高对数据安全事件的重视程度。中国在 2017 年正式开始实施《网络安全法》，目前国内物联网安全标准也已开始施行，摄像头安全风险在未来有待降低。

1.3.1 工业摄像头安全风险

对于工业方面使用的摄像头而言，一旦沦陷，首当其冲的危害就是大量的经济损失。早在 2014 年，俄罗斯和格鲁吉亚战争爆发前夕，一条由里海通向地中海的长 1099 英里的输油管在土耳其东部的位置突然发生爆炸，直接原因是输油管管内压力太大。令人费解的是，这条管道安装了大量的探测器和监控摄像头，但管理人员不仅在油管爆炸前未接收到任何关于这些设备的警示，事后也是从工人口中得知此事。随后，经过专业人员调查发现，这些监控摄像缺少了爆炸前后将近 60 个小时的录像，而在输油管较远的摄像头录像中则发现了两个身着军装的可疑人员对着笔记本电脑不停操作的画面。最后，此事件被定性为某国家的渗透行为，并且疑似早在 2008 年就开始布局，比美国对伊朗核反应堆发动的“震网计划”还要早。

图 1-5 某工业摄像头

1.3.2 公共摄像头安全风险

机场、景区、银行、停车场等公共场合布置的摄像头多出于安保的目的。与家庭摄像头相比，这类摄像头性能更高、覆盖面更广，一旦被黑客成功控制将对公共安全造成巨大威胁。通过这类摄像头，黑客不仅可以进行挖矿和 Dos 攻击，还有可能大范围、多角度地监视他人。这些监控摄像头往往位于开放式空间，任何攻击者都可以轻松了解其品牌和种类，然后“对症下药”。此外，不少公共摄像头在连接执法机构远程控制端的过程中，都需要经过多个中转点。这期间，如

若有一个中转点被黑客攻破，就会对整个系统造成巨大的安全危害。攻击者可通过传输节点，控制执行机构所能接收到的监视画面，出现好莱坞电影中描述的“黑客随意控制全城摄像头红绿灯”的场景。当电影画面成为现实，公共安全将受到的危害自然不言而喻。

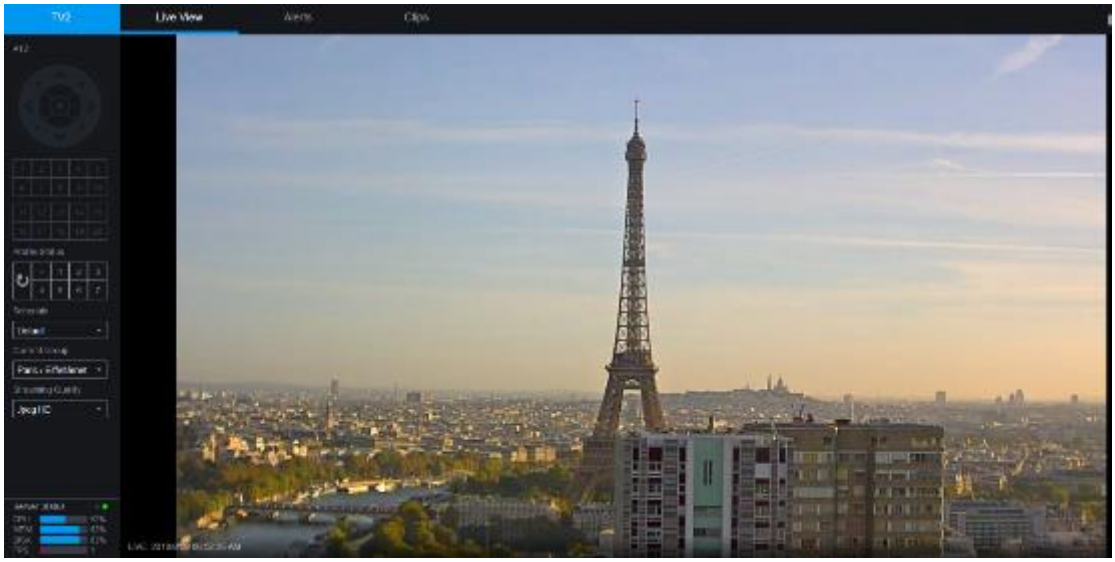

图 1-6 疑似埃菲尔铁塔附近摄像头

1.3.3 家庭设备安全风险

图 1-7 某室内摄像头

对于家庭摄像头设备，普通用户一般把摄像头部署在家里，用来监控孩子、宠物或店铺等。这类摄像头一旦被攻破，首先就会造成视频外泄，引发隐私问题，

一些倒卖此类非法视频的黑产也由此而生。在某些非法视频网站往往能看到这类视频的踪迹，售卖者以对某些人群满足生理和心理欲望的极具诱惑力的词汇作为视频标题，吸引相关人群来购买。其次，一旦家庭摄像头被控制，那么黑客就可以畅通无阻地以摄像头为跳板，攻击家庭范围内的其他物联网设备（电饭煲、冰箱、电灯、门锁等）和电脑手机等智能设备。而家庭网络往往由一台路由器管控，一旦攻击者入侵，可以说是无往不利。与室外公共网络设备相比较，人们通常会对家庭里的网络设备有更高的信任度，受害者在短时间内很难察觉有黑客入侵。攻击者利用这些设备既可进行挖矿和 DOS 攻击等非法获利行为，也可对家庭进行长期监控，严重威胁家庭生态安全。

2 摄像头暴露情况

现在的智能摄像头出于远程操控，因需向云服务上传监控视频，自动更新软件等使用需求，必须时刻和网络连接。正常摄像头的管理都处于内部网络中，外部无法访问，但仍有很多因素导致摄像头对外部开放，并暴露在互联网中。一是由于跨地域的摄像头管理需要开放摄像，如通过路由将摄像头的相关端口映射到外网中；二是用户仅考虑可用性，由于错误的配置导致直接外网可以访问。无论是有意或无意，这些摄像头直接公开在互联网中，任何连接到互联网的人都可以访问到这些摄像头的设备。通过对全球的公网 IP 进行常用端口扫描，再配合摄像头端口指纹进行识别，就可以了解全球摄像头设备的分布情况。对外暴露的摄像头存在巨大的潜在风险，恶意的攻击者通过漏洞或弱口令等即可实现恶意的攻击。以下是 FOFA 平台对全球摄像头设备暴露在外网的情况进行的详细分析。

2.1 摄像头全球各国家暴露情况

图 2-8 全球各国家摄像头暴露情况 世界地图

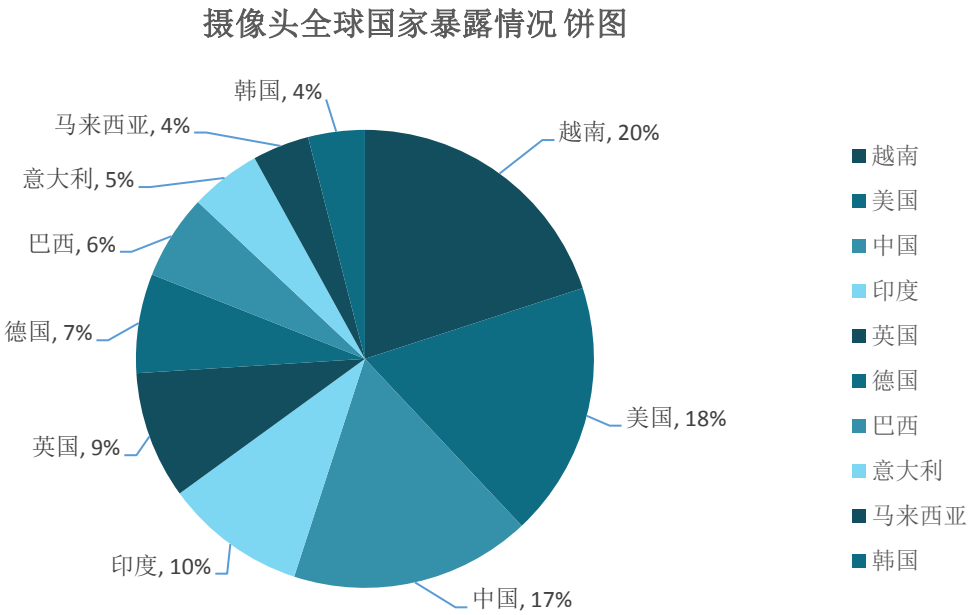

图 2-9 全球各国家摄像头暴露情况 饼图

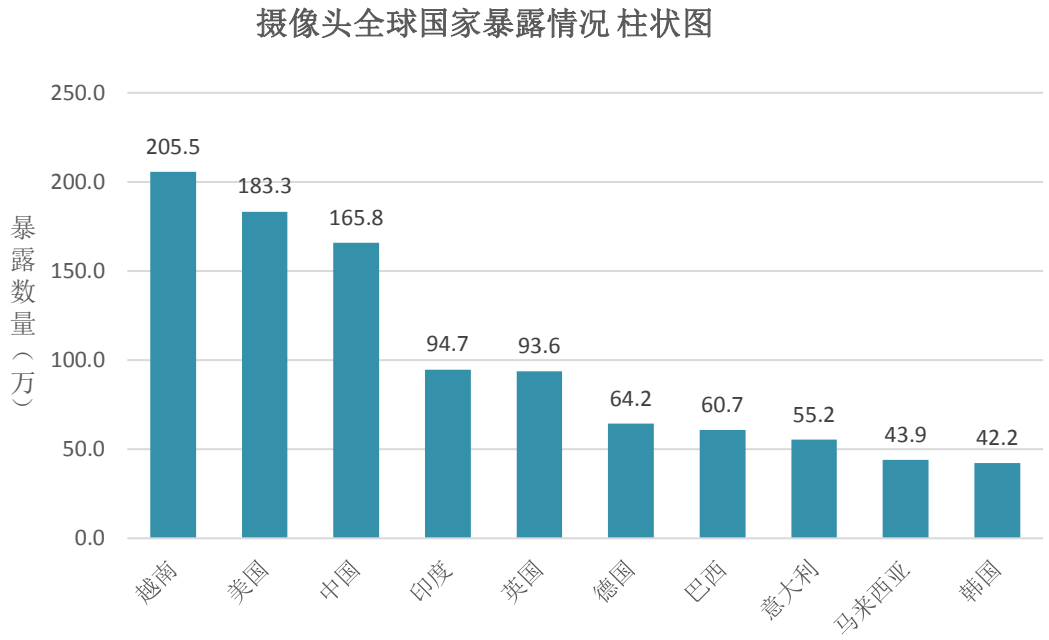

图 2-10 全球各国家摄像头暴露情况 柱状图

根据 FOFA 系统数据显示，截至 11 月底，全球共有 228 个国家 8063 个城市中的 2635 万摄像头设备对公网开放访问权限。其中越南位居第一，共有 205 万，约占 20%；美国位列第二，共有 183 万，约占 18%；中国位列第三，共有 165 万，约占 17%；印度共有 95 万，约占 10%；德国共有 94 万，约占 9%。(注:饼图中显示比例是 top 10 中所占比例，下文饼状图数据皆同上，后不予赘述)。

白帽汇安全研究院认为，摄像头对公网开放的安全问题已是全世界共同面临的重要挑战。其中，越南、印度因近年快速崛起而安全防护跟进滞后，使得视频监控设备在公网的暴露数量快速增加。美国、德国、中国、英国等也存在大量视频设备在公网暴露的情况。

2.2 摄像头全球各城市情况

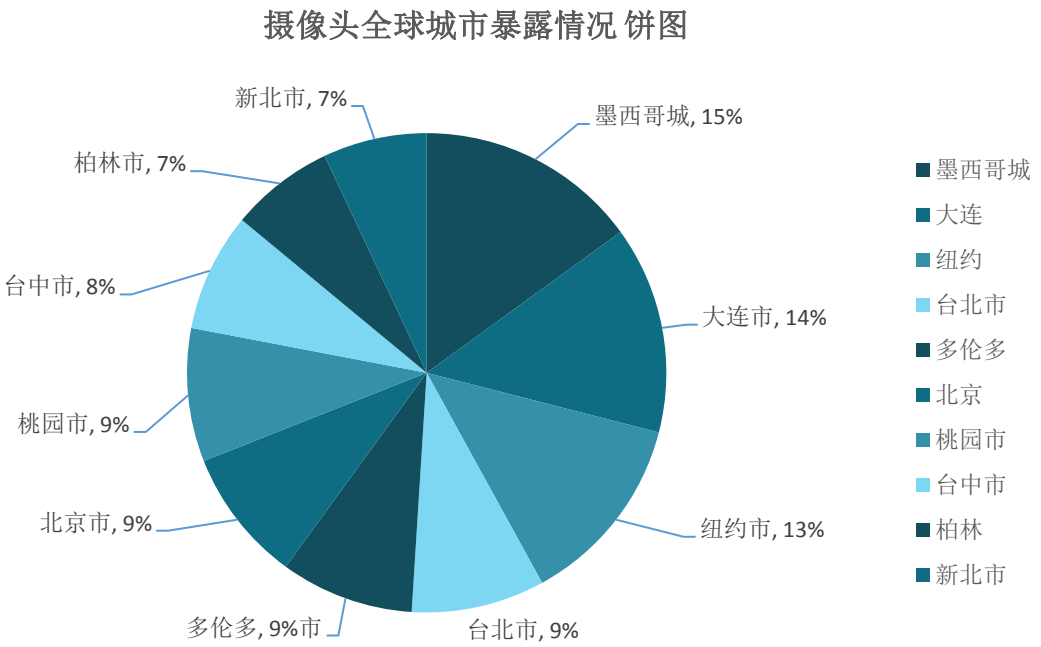

图 2-11 全球各城市摄像头暴露情况 饼图

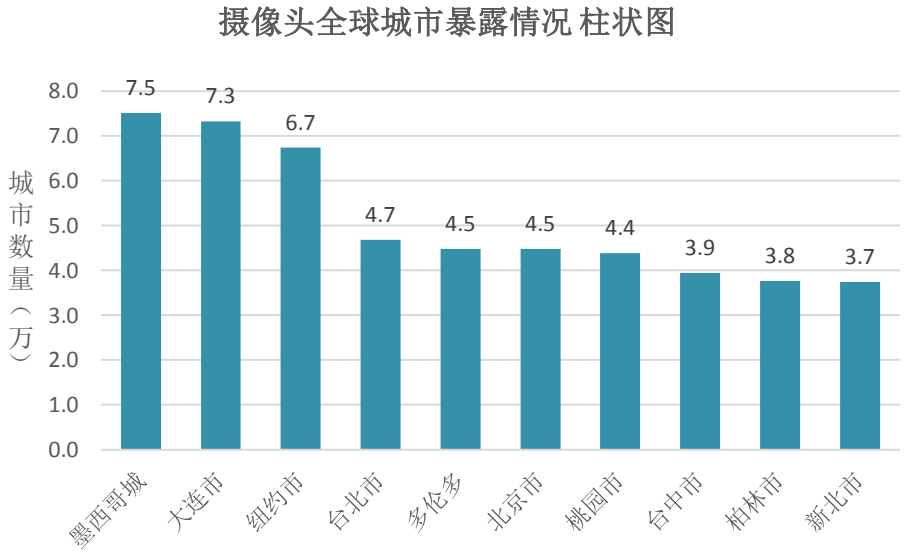

图 2-12 全球各国家摄像头暴露情况 柱状图

根据 FOFA 系统数据显示，全球共有 8063 个城市实现了摄像头设备的网络公开。其中墨西哥城最多，共有 7.5 万台设备，约占 15%；大连市位居第二，共有 7.3 万台设备，约占 14%；纽约位居第三，共有 6.7 万台设备，约占 13%；台北市位居第四，共有 4.7 万台设备，约占 9%；多伦多位居第五，共有 4.5 万台设备，

约占 9%。

不难发现，墨西哥城、大连、纽约、台北、多伦多无一例外是各国的政治、经济、文化和交通中心。以墨西哥城为例，它是美洲人口最多的都市区，集中了全国约 1/2 的工业、商业、服务业和银行金融机构。正是由于城市的功能特征，使得视频监控设备在网络公开的数量规模呈现出空前巨大的现状。

2.3 摄像头中国大陆各省情况

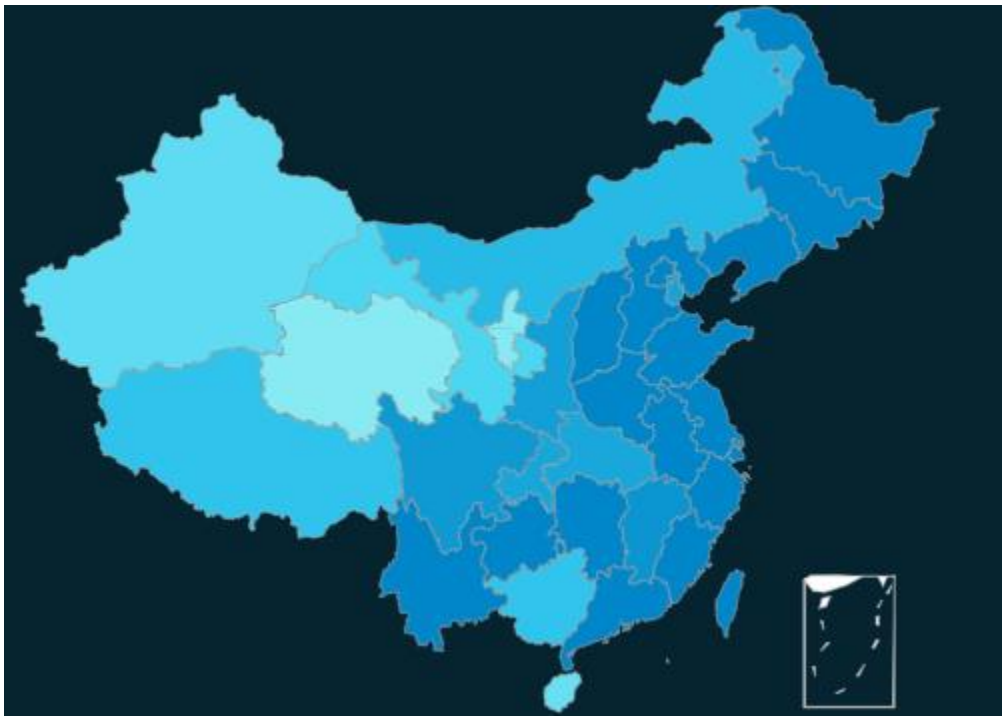

图 2-1 摄像头中国大陆各省暴露情况

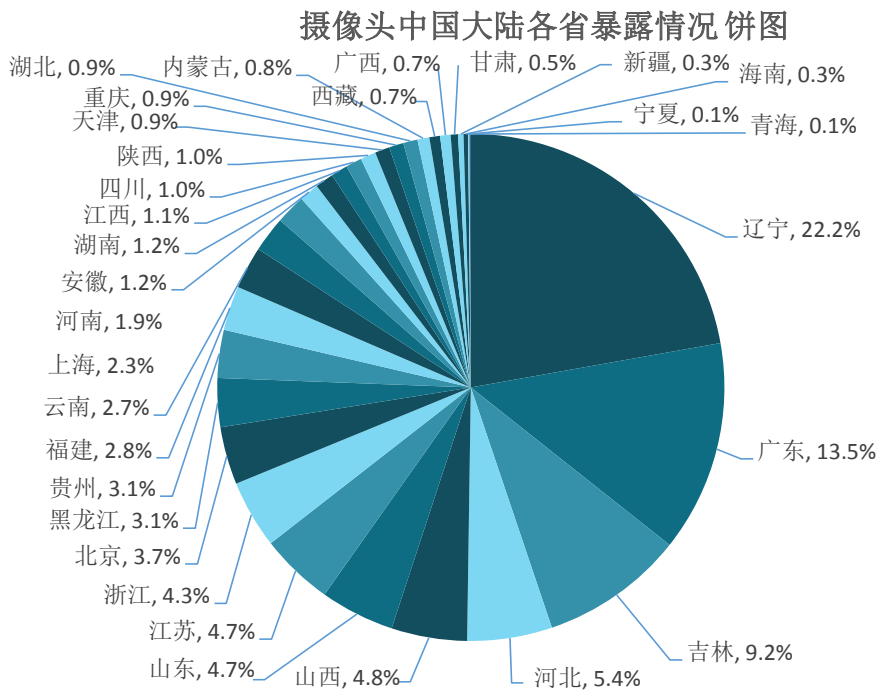

图 2-2 中国大陆各省摄像头暴露情况 饼图

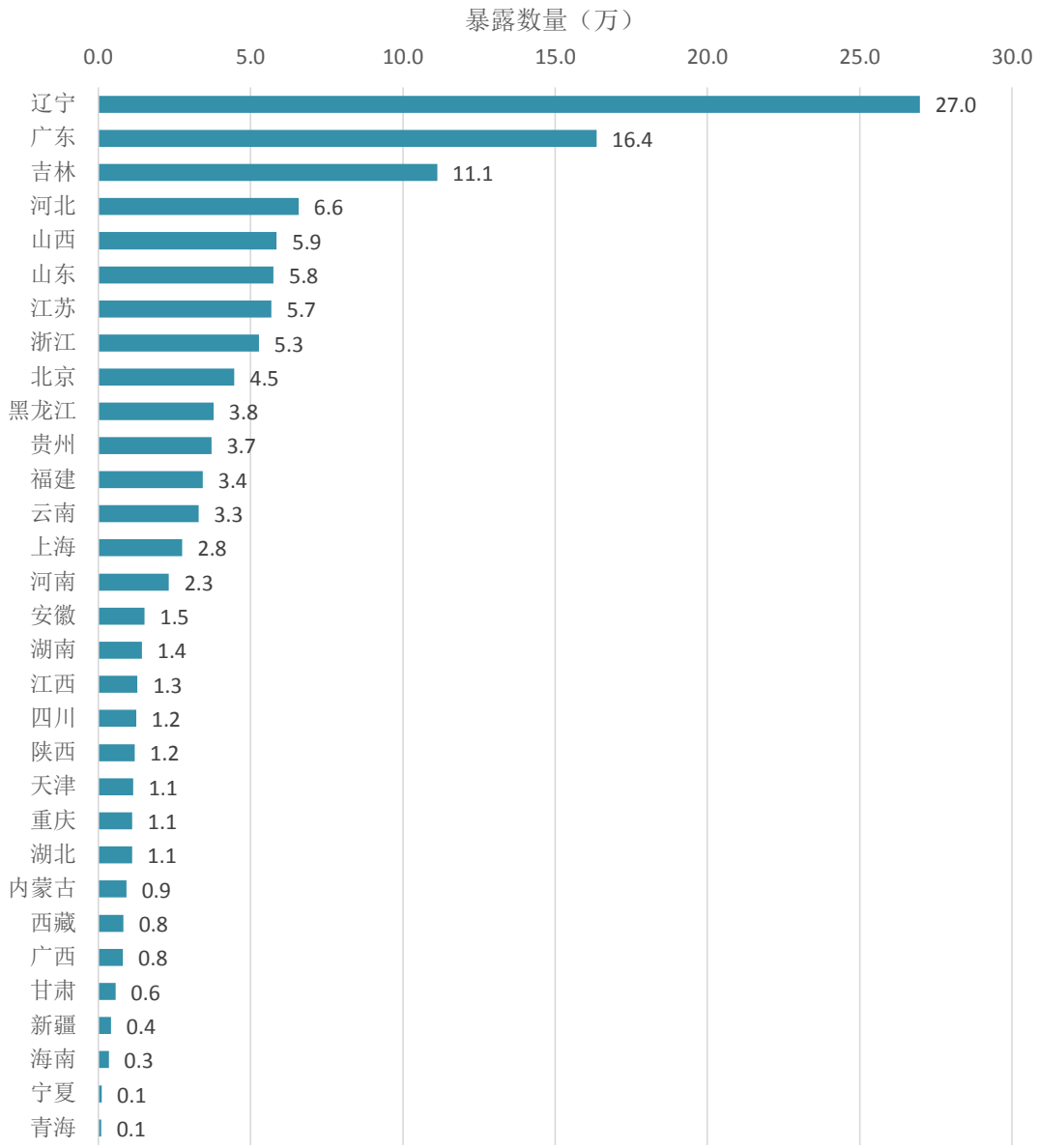

图 2-3 中国大陆各省摄像头暴露情况 条形图

根据 FOFA 系统数据显示，辽宁省暴露最多，共有 27 万台设备，约占 22%；广东省第二，共有 16.4 万台设备，约占 14%；吉林省第三，共有 11.1 万台设备，约占 9%；河北省第四，共有 6.6 万台设备，约占 5%；山西省第五，共有 5.9 万台设备，约占 5%。

2.4 摄像头中国各城市情况

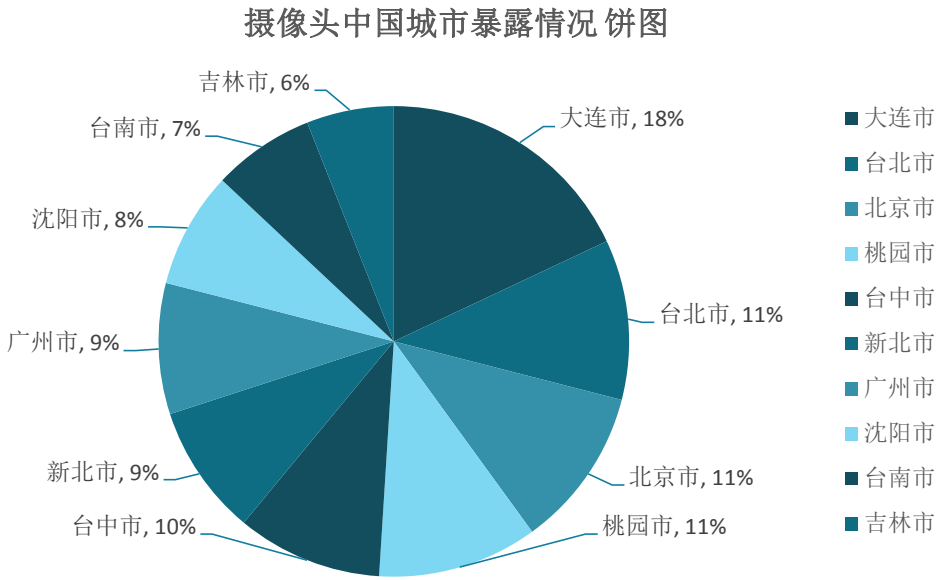

图 2-4 中国各城市摄像头暴露情况 饼图

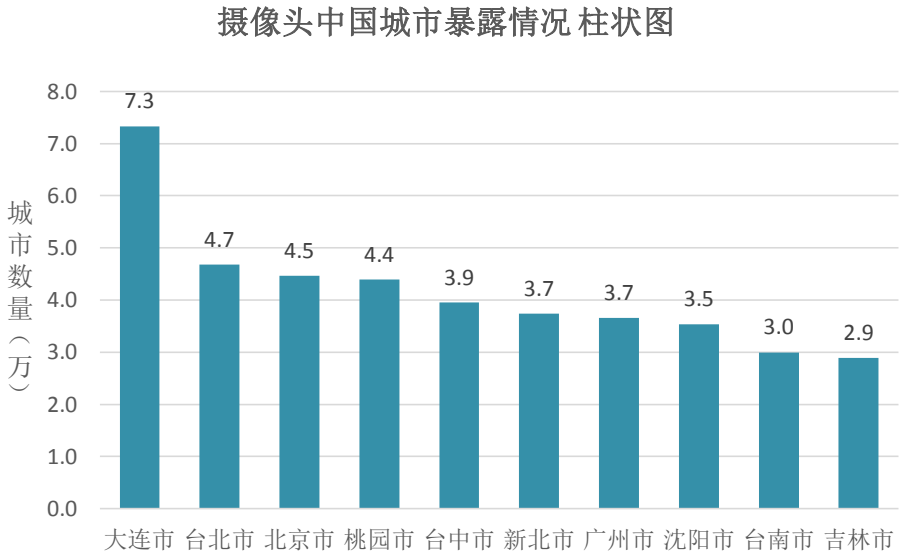

图 2-5 中国各城市摄像头暴露情况 柱状图

根据 FOFA 系统数据显示，中国共有 385 个城市实现了摄像头设备的网络公开。其中大连市最多，共有 7.3 万台设备，约占 18%；台北市第二，共有 4.7 万台设备，约占 11%；北京市第三，共有 4.5 万台设备，约占 11%；桃园市第四，共有 4.4 万台设备，约占 11%；台中市第五，共有 3.9 万台设备，约占 10%。

由此数据可以看出，摄像头设备在网络公开的中国城市中，绝大部分为中国的一线城市、经济中心和人口密集城市。

2.5 摄像头中国港澳台暴露情况

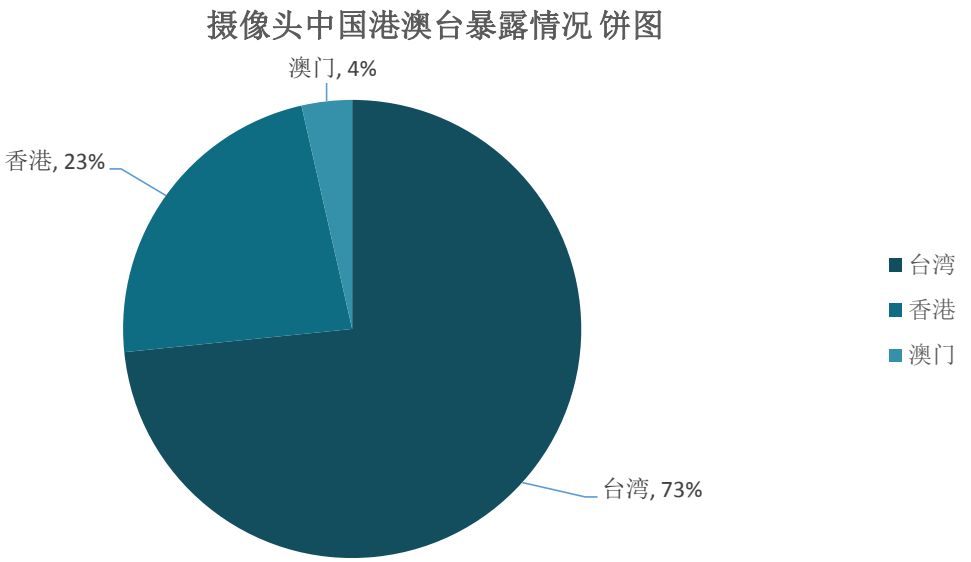

图 2-6 中国港澳台摄像头暴露情况 饼图

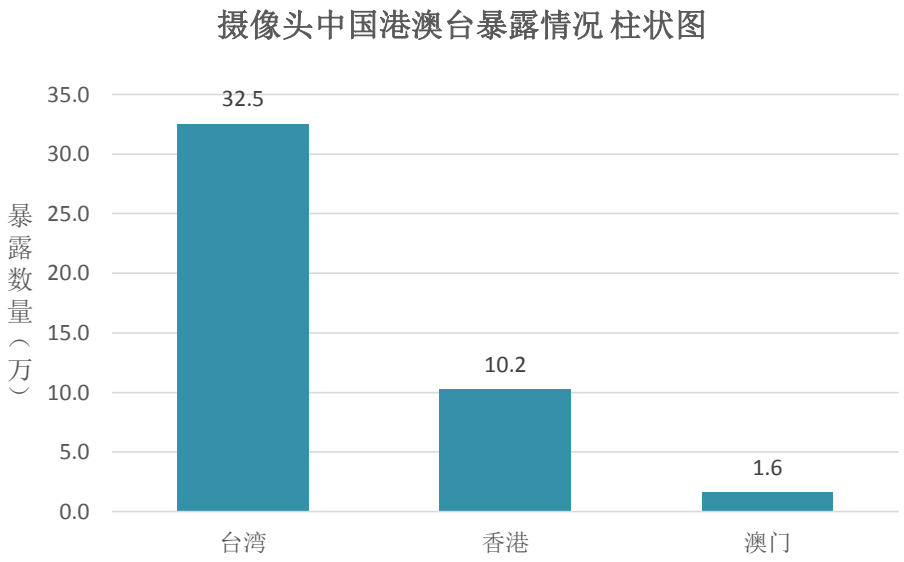

图 2-7 中国港澳台摄像头暴露情况 柱状图

根据 FOFA 系统数据显示，中国港澳台地区台湾省最多，共有 32.5 万台设备，占港澳台总数的 73%；第二是香港，共有 10.2 万台设备，占港澳台总数的 23%；澳门第三，共有 1.6 万台设备，占港澳台总数的 4%；

2.6 摄像头全球暴露的产品分析

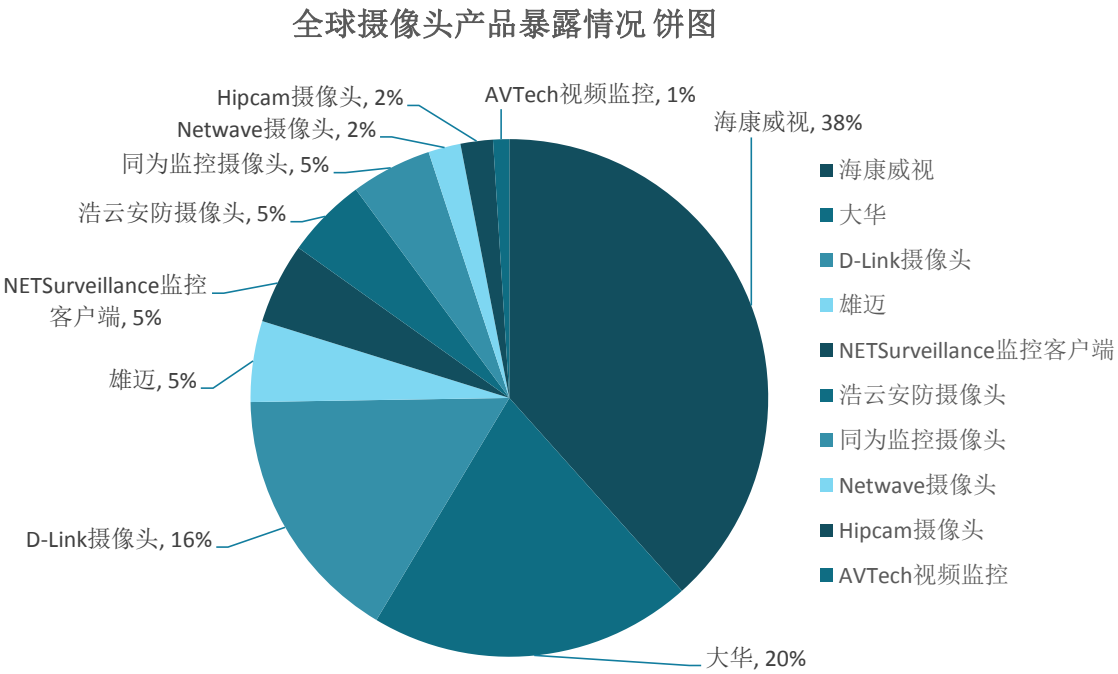

图 2-13 对外暴露摄像头厂商 饼图

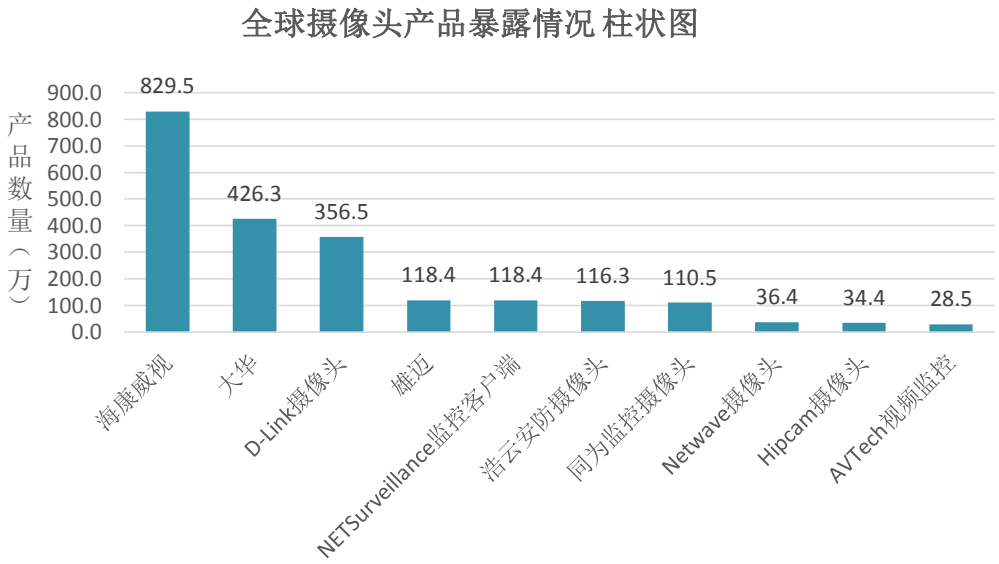

图 2-14 对外暴露摄像头厂商 柱状图

根据 FOFA 系统统计显示，摄像头目前网络公开最多的为海康威视，共 829 万台，约占 38%，第二为大华摄像头，共 426 万台，约占 20%，第三为 D-Link 网络摄像头，共 356 万台，约占 16%，第四为雄迈，共 118 万台，约占 5%，第五为 NETSurveillance，共 118 万台，约占 5%。

2.7 摄像头暴露端口和协议分析

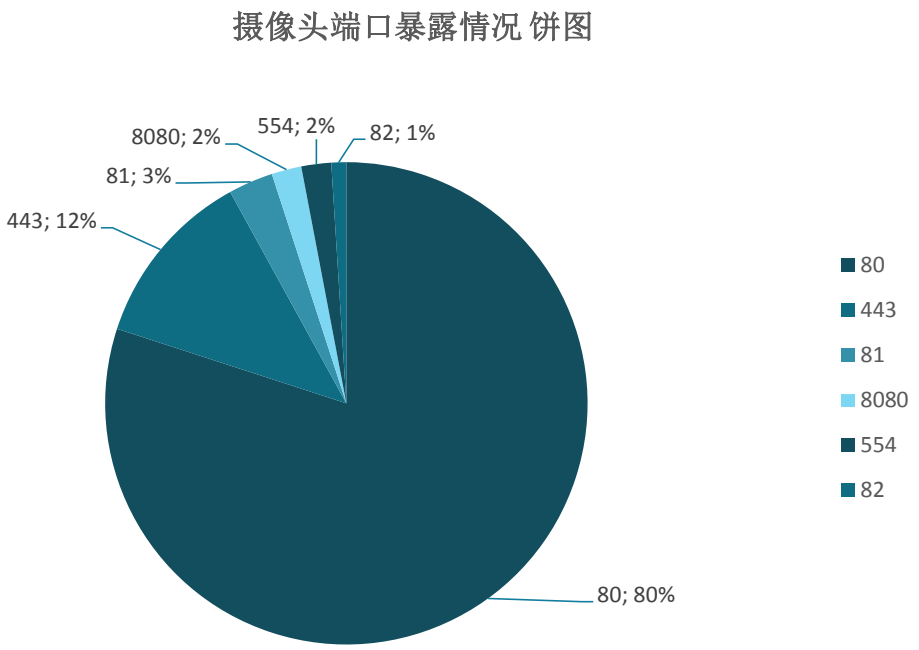

图 2-15 摄像头端口暴露情况 饼图

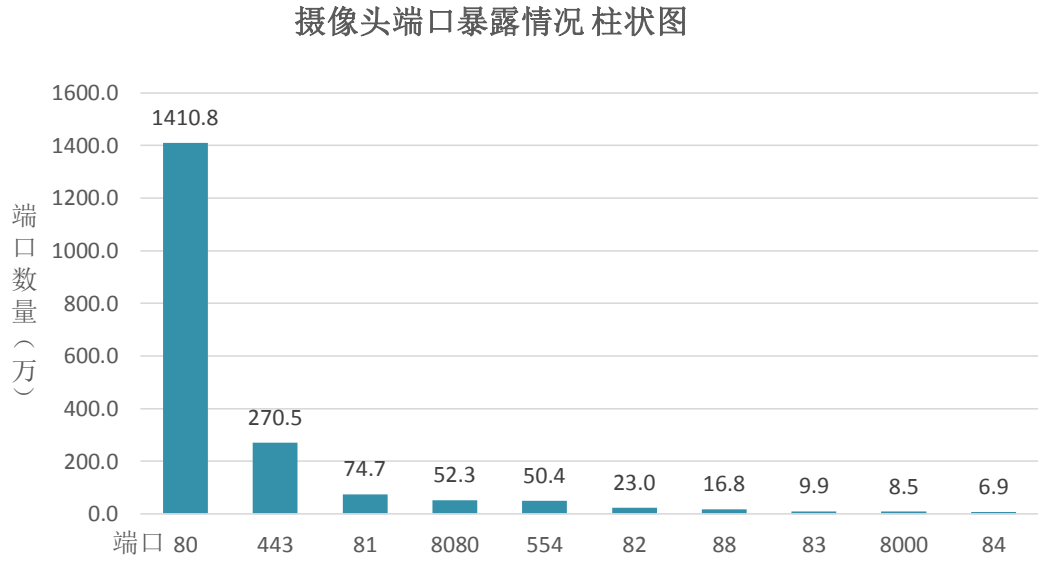

图 2-16 摄像头端口暴露情况 柱状图

就摄像头设备被公布在网络中的端口而言，80 端口数量最多，共有 1411 万，约占 80%，443 端口第二，共有 270 万，约占 12%；81 端口第三，共有 75 万，约占 3%，8080 端口第四，共有 52 万，约占 2%；554 端口第五，共有 50 万，约占 2%；其他端口约占 1%。

Web 服务的默认访问端口为 80 和 443，80 端口对应标准协议为 http；443 端口对应标准协议为 https；81 和 8080 端口大部分也是 http 或 https 协议。由此可看出，目前主流的摄像头都提供 Web 管理接口。除此之外，554 端口默认对应 rtsp 协议，rtsp 作为实时流传输协议，是摄像头视频流传输的主要应用协议。

通过对端口和协议的分析，我们发现，目前互联网中的 80%摄像头未采用加密传输，摄像头内容存在被窃听、被篡改等安全风险。

3 摄像头安全问题

3.1 摄像头安全漏洞

3.1.1 漏洞类型

摄像头设备存在的漏洞类型包括权限绕过、拒绝服务、信息泄漏、跨站、命令执行、缓冲区溢出、 SQL 注入、弱口令、设计缺陷等。

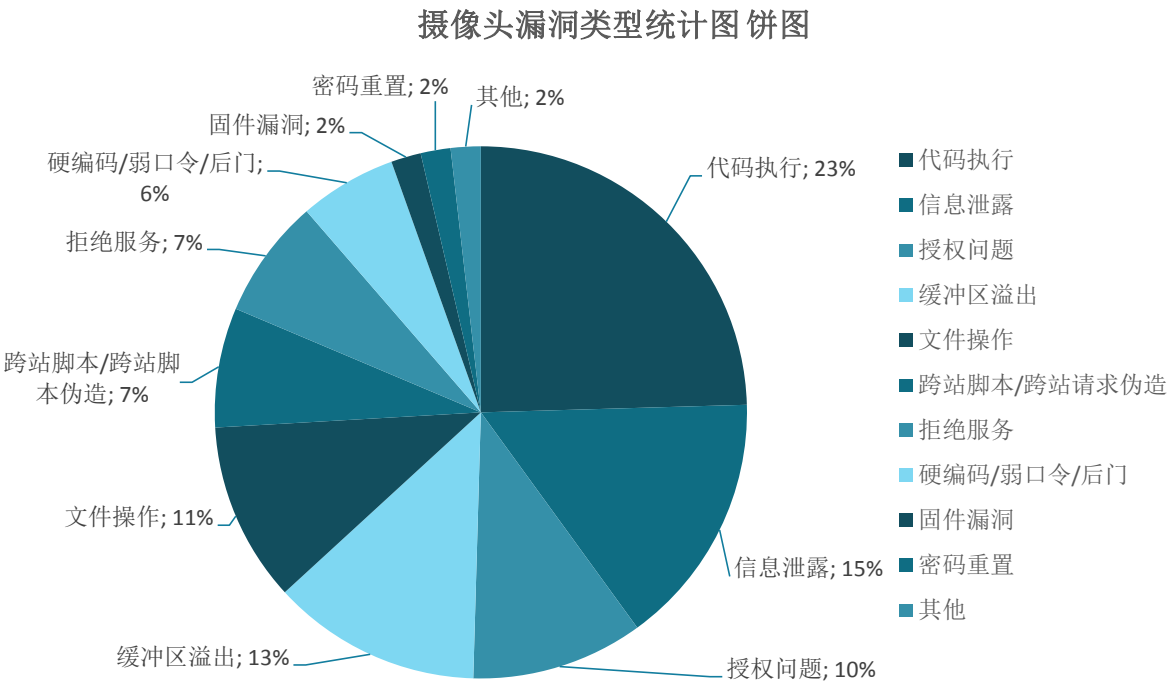

图 3-1 2018 年漏洞类型统计 饼图

漏洞类型	危害	数量（2018 年）
命令注入	可执行系统命令或任意代码	46
授权问题	可未授权访问设备	41
信息泄漏	可泄漏用户凭证，RTSP 流，实时图像等敏感文件	29
缓冲区溢出	可使系统崩溃或重启，甚至可能利用它执行命令，获得系统权限	24
硬编码/弱口令/后门	可直接进入设备，控制设备	20
文件操作	可下载、读取、修改、上传、删除任意文件	14
XSS	可窃取用户 cookie，读取用户数据等	13
拒绝服务	造成内存损坏和崩溃，使设备无法提供正常服务	9
目录遍历	可查看系统目录、读取任意文件等	8
固件漏洞	固件降级、不安全固件更新方式、固件恢复、固件升级	6
CSRF	可更改管理员证书或创建新的用户	4
重置/修改账户	可重置或修改任意账户密码等设置	3
重定向	有利于攻击者发动钓鱼攻击	1
sql 注入	数据库泄漏，威胁系统安全	1
xml 实体注入	可造成敏感信息泄漏	1

表 3-1 2018 年摄像头漏洞各种类型危害及数量

其中，权限绕过、信息泄漏、代码执行漏洞数量占比最高，分别占所有漏洞类型总数的 23%、15%和 10%。代码执行漏洞的危害与影响最大。恶意攻击者可以通过该漏洞执行植入僵尸程序，达到完整控制该程序的目的。此外，摄像头设备授权验证等也是一个较大的问题，若出现漏洞将直接导致用户隐私数据遭到泄漏。值得关注的是，硬编码\默认密码\隐藏后门等占比 6%，此类漏洞可能是厂商或厂商被攻击者入侵，而在设备中制造的后门。通过后门，摄像头厂商或者恶意攻击者可以直接控制设备，对用户隐私内容的安全防护来说是一个巨大的威胁。

3.1.2 历年漏洞

白帽汇安全研究院根据 CNNVD、CVE 和 FOFA 平台的不完全统计，对近六年摄像头的漏洞数量分布进行分析显示：摄像头漏洞数量总体呈上升趋势。

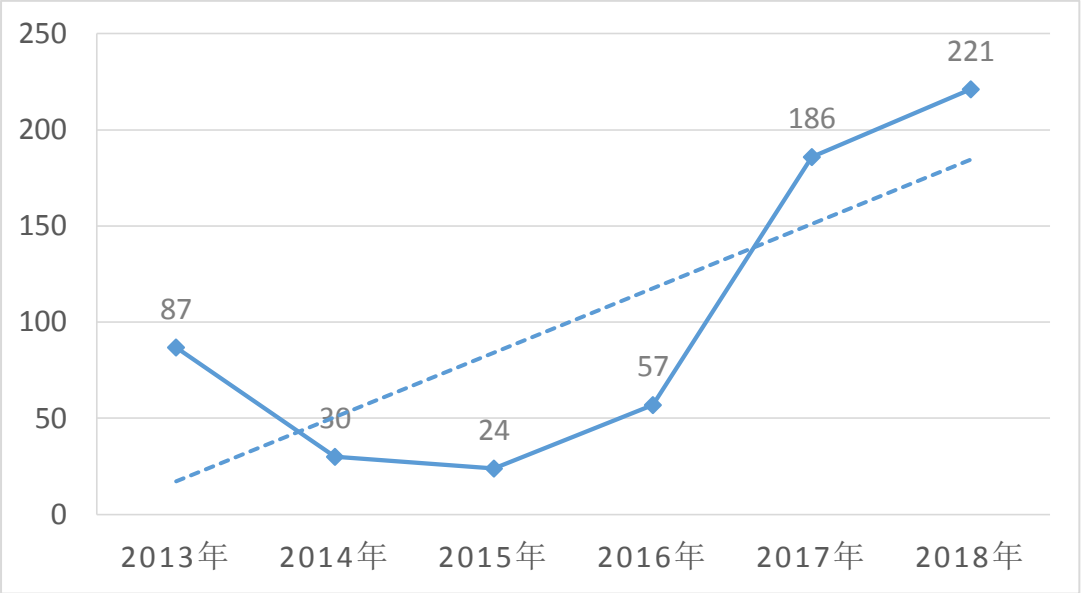

图 3-2 摄像头漏洞近六年分布图

据调查分析，2013 年监控摄像头在民用市场的数量暴增，摄像头漏洞也随之迅速增长。2013 年曝光的漏洞主要有 Hikvision、Samsung、D-Link、Lorex、Cisco、Foscam、Vivotek、Zavio、TP-Link、MayGion、QNAP、Brickcom、Sony、Grandstream、Ovislink、Airlink、 Avtech 和大华等厂商。2014 年—2016 年摄像头漏洞以年均不到 40 个的速度开始下降；而 2017 年又开始呈现出爆发式增长的趋势，仅 2017 年一年就公开了 186 条左右漏洞；截止至 2018 年 11 月，2018 年公开发布的摄像头漏洞达 221 条以上，比去年增长了 19%。

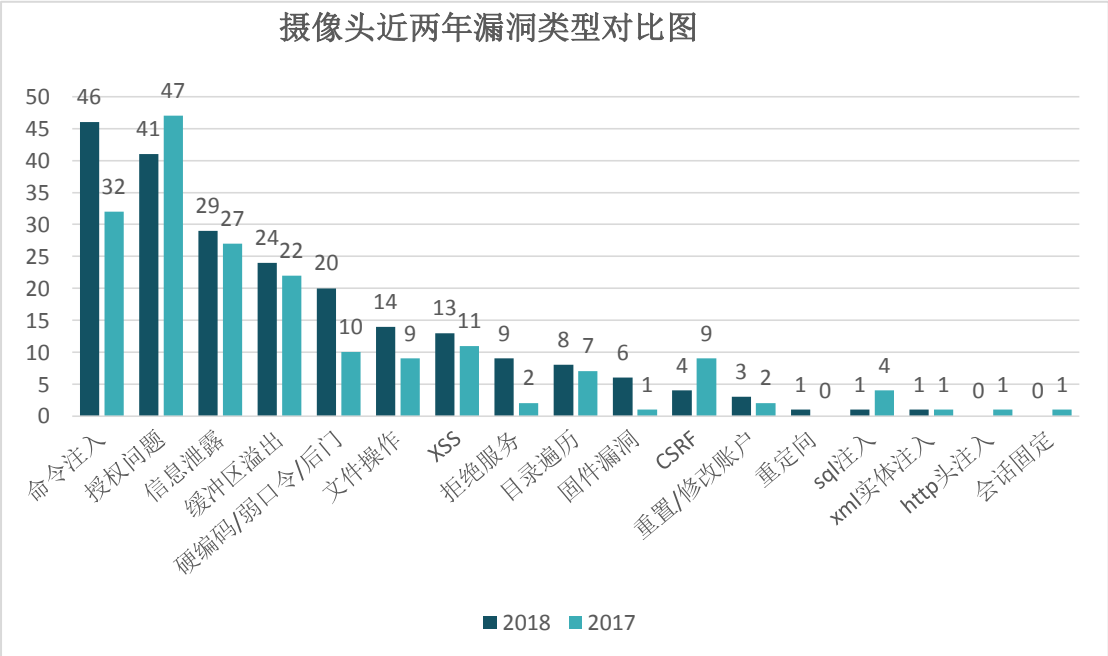

图 3-3 漏洞类型近两年对比图

2018 年与 2017 公布的漏洞类型相差无几。2018 年命令执行漏洞最严重，达 46 个以上，占漏洞总数的 21%，2017 年则大约 32 个左右，占漏洞总数的 17%；2017 年授权漏洞最严重，达 47 个以上，而 2018 年 41 个以上，与 2018 年相差不大；信息泄漏的漏洞 2017 年与 2018 年只相差 2 个，分别为 27 和 29 个。其中命令执行漏洞危害最大，攻击者可以直接执行系统命令或读写文件反弹 shell，控制整个设备甚至控制服务器，进一步渗透至内网等。信息泄漏漏洞则是通过用户名密码、RTSP 流、实时图像等高度敏感文件的直接泄漏，攻击者能够轻易控制整个设备，直播摄像内容，泄漏客户隐私。

自摄像头被广泛应用以来，各大摄像头厂商公布的漏洞数量始终居高不下。其中，中国深圳市福斯康姆智能科技有限公司（Foscam）在 2017 年公布的摄像头漏洞高达 52 个，其中多为命令执行、缓冲区溢出、授权问题、硬编码、信息泄漏等漏洞。下图为部分厂商 2017 年-2018 年漏洞数量对比图。

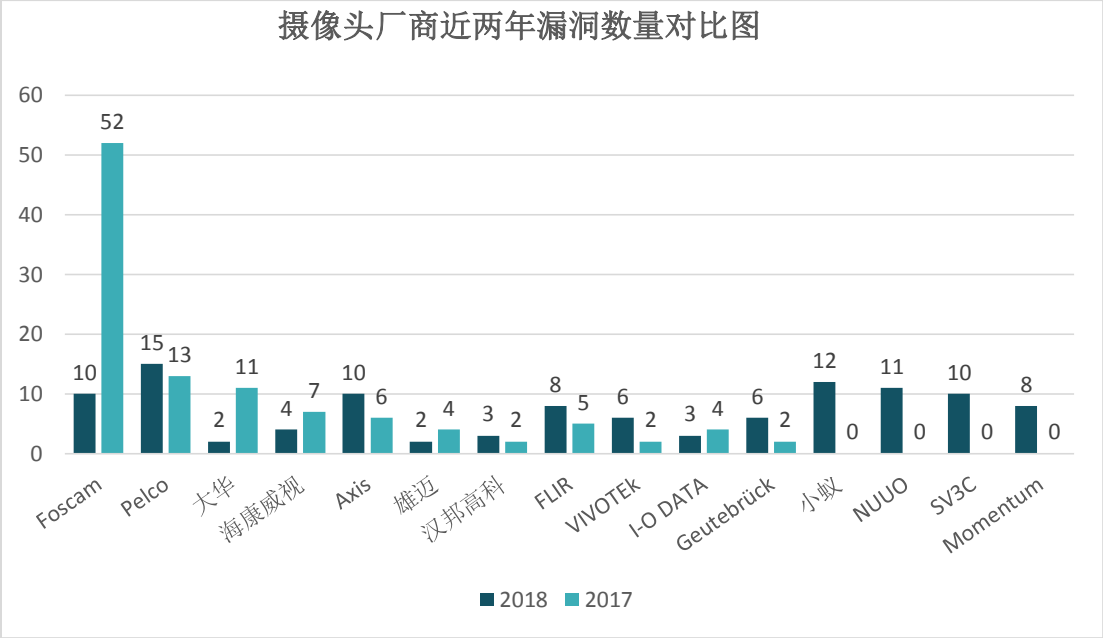

图 3-4 摄像头厂商近两年漏洞数量对比图

根据 FOFA 平台的抽样检测显示，数年前公布的漏洞现在依然存有较大的漏洞率。如 2017 年 3 月在国外论坛上公布的一个海康威视摄像头漏洞，出于大众安全的原因，海康威视要求漏洞发现者延迟披露漏洞信息。直到这个漏洞 9 月份在国内曝光时，国外几乎已经全部完成了修复，而国内漏洞率仍高达 30%。对于总量高达 2635 万的摄像头来说，这个漏洞率是十分可怕的。2017 年，由深圳市

丽欧（Neo）电子有限公司生产的超过 175,000 台物联网摄像机由于设备访问协议中的基本漏洞，曝出了可远程访问和查看的漏洞。危害风险波及全球，直到现在，该摄像头漏洞率仍高达 15%。同年，大华摄像头被曝存在预留后门，大华厂商很快发布了固件更新，但直至今日，该摄像头仍有很大一部分（大约 3 万台左右）存在漏洞。

摄像头厂商一般会在漏洞公开一周内更新补丁，但由于大量物联网设备是经过不同的平台制造商进入市场的，因此在漏洞补丁公开后很难在第一时间有效地是实现不同的物联网设备和平台的信息发布和部署更新，再加上用户安全意识薄弱，对安全事件关注度较低。至此，设备得不到及时更新，而这也是导致漏洞率几年内依然居高不下的关键所在。

典型摄像头漏洞案例

- 雄迈云服务器内置硬编码账户漏洞（CVE-2018-17919）
- NUUO 摄像头最新高危漏洞预警(CVE-2018-1149)
- 数十万酷视网络摄像头存在高危风险，可导致视频泄漏
- Sony IPELA E 系列网络摄像头远程命令执行
- Axis 摄像头存在安全缺陷，三个漏洞即可接管
- 海康威视网络摄像头访问控制绕过漏洞
- 浙江大华摄像存在 0day 后门
- 浙江大华摄像头存在高危漏洞
- 国内 Foscam IP 摄像头被曝出大量漏洞
- 三星智能监控摄像头被爆远程代码执行漏洞
- D-Link 云摄像头超过 120 款产品存在漏洞，约 40 万台设备受影响
- CCTV 摄像头存在多个漏洞

3.1.3 曝光安全漏洞的摄像头厂商

目前被曝光过漏洞的摄像头品牌有 Hikvision(海康威视)、松下、SONY、Canon、Samsung、CCTV、TPLINK、LG、Trendnet-IP-Cam、MOLE、博视-DINION、Defeway、INTELLINET、大华、酷视 NEO、NUUO、Swann、Axis、Foscam、MasterIPCAM01、

MJPG-streamer、FLIR、RPi、Pelco、Brickcom、Webcam XP、biueiris、ABUS、Yawcam、Momentum、Mobotix、Argus Surveillance、SIEMENS、vstarcam(威视达康)、汉邦高科、Geovision、 StarDot、Trendnet、Sarix Pro、Vivotek、Digital Watchdog、Basler、Arecont Vision、ACTi、IP CAMERA LUPUS、Digoo 等。

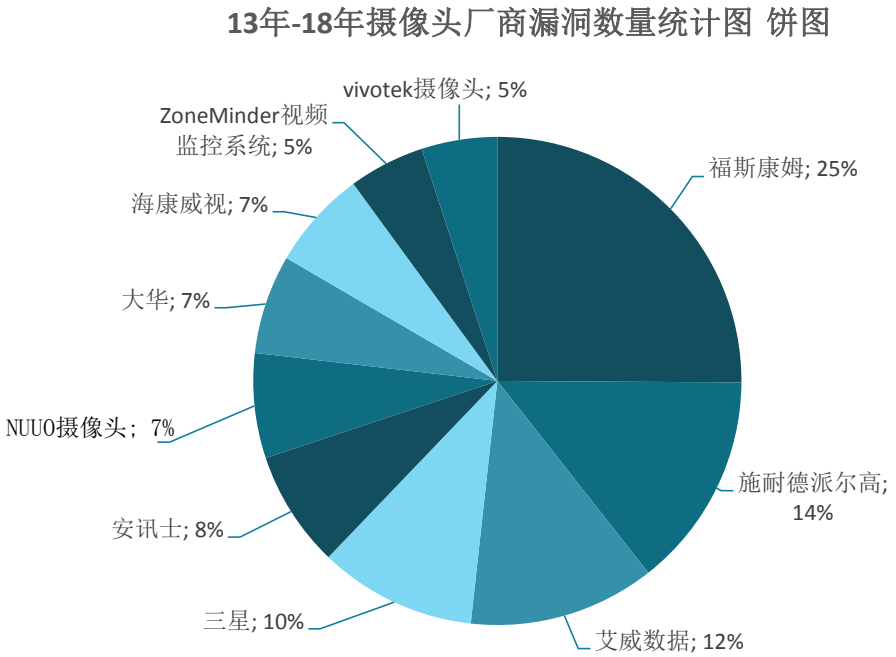

图 3-5 摄像头漏洞厂商分析 饼图

摄像头厂商	产品暴露总量	漏洞数量（个）
福斯康姆	24 万	65
施耐德派尔高	521	37
艾威数据	4	32
三星	35 万	27
安讯士	2.4 万	20
NUUO 摄像头	2.3 万	18
大华	426.3 万	17
海康威视	829.5 万	17
ZoneMinder 视频监控系统	1341	13
vivotek 摄像头	1.1 万	13

表 3-2 13 年-18 年摄像头厂商漏洞数量前 10

目前公开的摄像头漏洞中，涉及 hikvision、NUUO、Foscam、大华等厂商。其中，中国福斯康姆（Foscam）摄像头漏洞数量最多，达 65 条以上，占历年摄像头漏洞总量的 25%；法国施耐德旗下派尔高（pelco）摄像头漏洞数量位列第

二，达 37 条以上，占历年摄像头漏洞总量的 14%；日本艾威数据（I-O DATA）摄像头位列第三，达 32 条以上；韩国三星（Samsung）、中国安讯士（Axis）摄像头厂商分别位列第四和第五；浙江大华和中国海康威视（hikvision）摄像头分别位列第六和第七，漏洞数量达 17 条以上。

3.1.4 漏洞危害

常见的摄像头漏洞包括远程命令执行漏洞，任意文件读取漏洞，用户密码重置漏洞，未授权访问漏洞，登录绕过漏洞，存在隐藏后门等漏洞。这些漏洞任何一个都能给用户带来极大的安全风险，导致隐私信息泄漏。以下是几种高危漏洞的说明和展示。

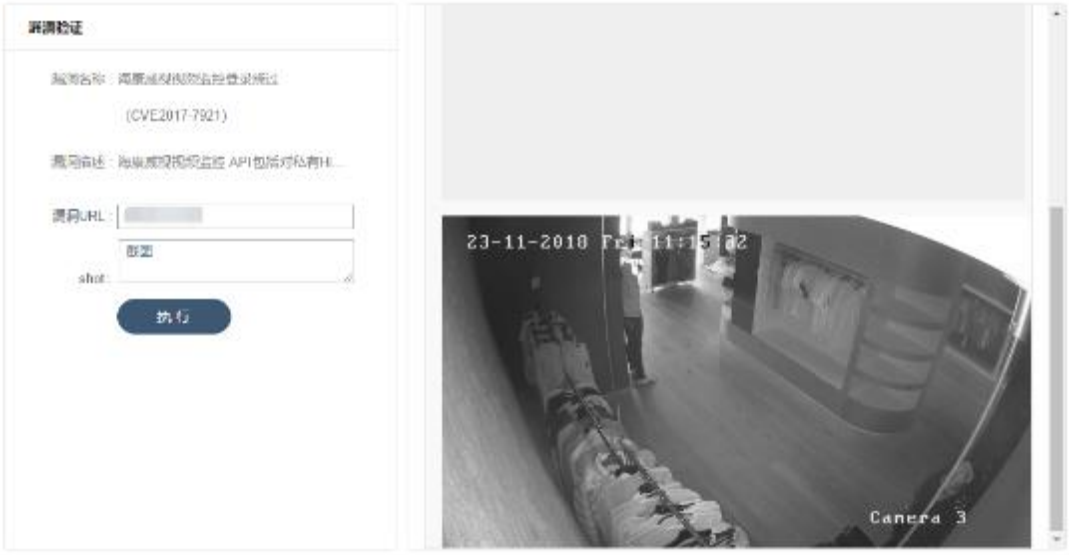

图 3-6 海康威视登陆绕过漏洞（CVE-2017-7921）

海康威视登陆绕过漏洞，利用该漏洞可以绕过海康威视摄像头的登录验证。其原理是因为海康威视视频监控 API 包括对私有 HikCGI 协议的支持，该协议通过摄像头的 web 界面公开 URI 端点。HikCGI 协议处理程序检查查询字符串中名为“auth”的参数是否存在，如果该参数包含 base64 编码的“user:password”的字符串，则 HikCGI API 协议调用伪装的用户身份，密码将被忽略。该漏洞可以直接获取用户密码配置和截图。可以在不登陆的情况下查看监控截图，上图是利用 FOFA 客户端进行的漏洞验证（本节截图仅为漏洞测试）。

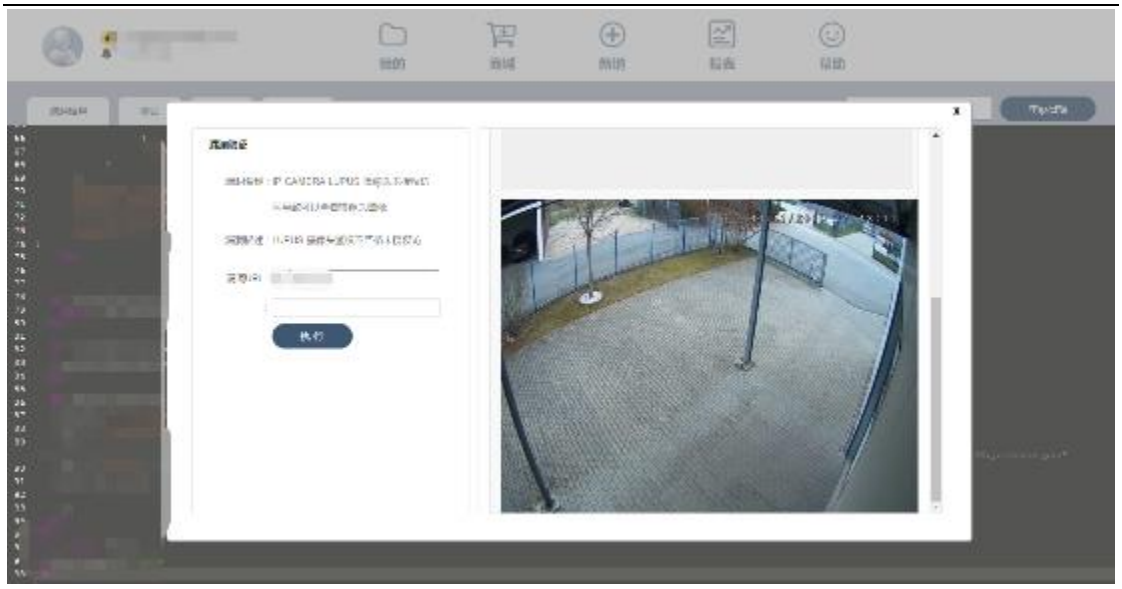

图 3-7 IP CAMERA LUPUS 摄像头未授权访问漏洞

IP CAMERA LUPUS 摄像头的未授权访问漏洞。未授权访问可以理解为需要安全配置或权限认证的地址、授权页面存在缺陷，导致其他用户可以直接访问，从而引发重要权限可被操作、数据库、网站目录等敏感信息泄漏。该摄像头的未授权访问漏洞是因为/GetImage.cgi 页面未添加合理的身份验证，导致可以不用登录查看监控摄像截图。

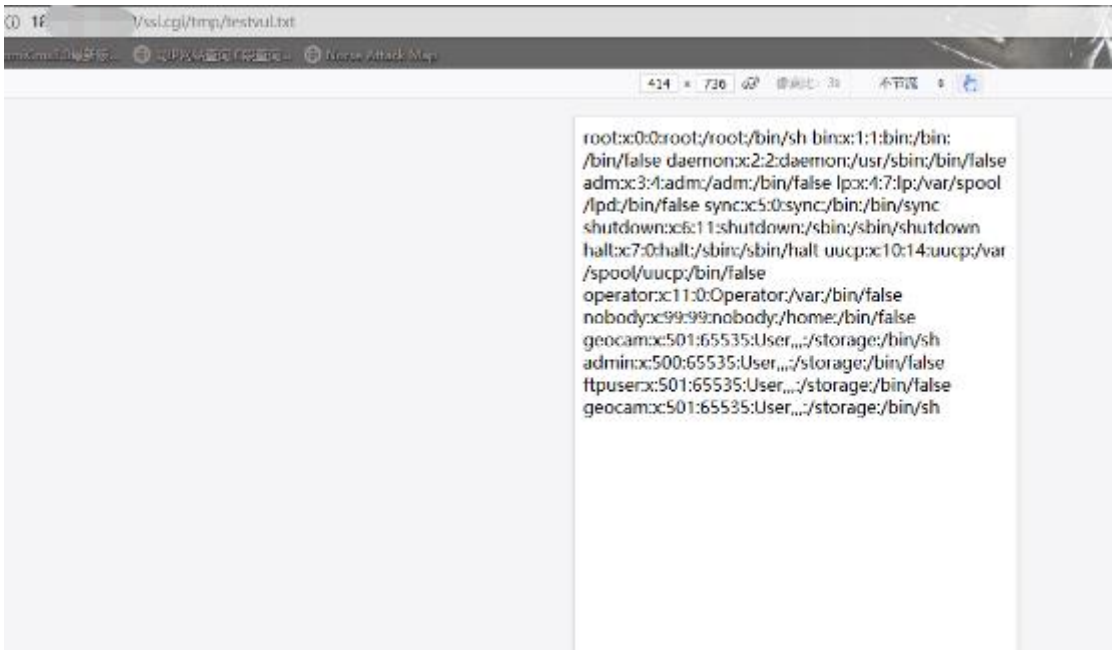

图 3-8 Geovision IP Camera 命令执行漏洞

Geovision IP Camera 命令执行漏洞。命令执行漏洞原理是当应用需要调用一些外部程序去处理内容的情况下，会用到一些执行系统命令的函数。并且当用

户可以控制命令执行函数中的参数时，将可注入恶意系统命令到正常命令中，造成命令执行攻击。利用该漏洞不仅可以看视频流，已经可以完全控制摄像头。

图 3-9 LG 智能摄像头 t.report 敏感文件下载

LG 智能摄像头敏感文件下载漏洞。其软件版本小于 1508190 时，存在敏感文件泄漏问题，该漏洞产生原因也是访问权限控制不严格，导致攻击者可以在未授权的情况下，下载日志文件 t.report,其中包含了软件版本和配置信息，攻击者可借此展开下一步攻击。

3.2 未授权访问

未授权访问指的是在没有预先得到许可的情况下，利用摄像头设备的安全配置以及权限认证出现缺陷的情况，非法进入摄像头设备，浏览管理界面。未授权访问广泛存在于各个安全领域，智能摄像头则更甚。

比如利用 RTSP 协议的未授权访问查看摄像头的视频流或实时监控截图，导致用户的隐私生活暴露在众目睽睽之下。还有未经授权查看设备的配置信息或管理界面等，攻击者可以获取摄像头设备的配置信息，比如用户名密码等，或者进入管理页面修改摄像头的相关配置，从而获得摄像头的控制权限。

目前统计，许多摄像头都曝出过未授权访问漏洞，而且此类漏洞利用方法都比较简单，但是危害却很高。比如 SONY 网络摄像头未授权访问漏洞、Geovision IP Camera 未授权读写漏洞，TPLINK-摄像头未授权访问漏洞，博世-DINION IP 摄像头未授权访问，Defeway 摄像头未授权访问漏洞，FLIR 摄像头存在未授权访

问漏洞，ABUS 网络视频摄像头未授权访问漏洞，Yawcam 摄像头未授权访问漏洞等。此类漏洞频繁爆发，厂家应该重视此类问题。

在 2014 年的时候，全球顶级的摄像头厂商 AXIS 就曾曝出未授权访问事件，任何人只需要输入特定的 url 路径，就可以直接实时查看监控视频，中间没有任何身份验证和警告措施。

而在 2017 年，我国大华摄像头也被曝出未授权访问漏洞，该漏洞不是通过 80 端口，而是通过访问设备的 37777 端口就可以直接看到监控视频。现今公网上开放的大华设备经 FOFA 统计大概有两百万台，存在未授权访问的机器即使只有百分之一，也影响了近两万设备。

图 3-10 某学校学生正在上课的监控画面

图 3-11 某高中学生上课监控画面

图 3-12 某银行监控画面

图 3-13 某机关单位监控画面

3.3 默认口令

目前绝大部分的摄像头管理都存在默认口令，默认口令是设备出厂的默认密码。在现实生活中，许多用户并不会、也不会想到对默认口令进行修改。这将导致暴露在互联网中的摄像头存在着大量的默认口令，攻击者通过收集这些口令，

对全网的摄像头设备进行暴力破解，即可获取大量摄像头信息。这一漏洞的存在将为恶意攻击者提供了极其简单、成本低廉但危害巨大的攻击方式。据了解，目前网络售卖的个人隐私视频采用的主要方法就是默认口令。

僵尸网络里大部分是 IoT 设备，比如 Mirai，Mirai 僵尸网络控制着数以百万计的物联网设备，其中摄像头设备占了很大比重。Mirai 恶意程序通过扫描物联网设备，尝试默认通用密码进行登录操作，一旦成功即将这台物联网设备作为“肉鸡”纳入到僵尸网络里，进而操控其攻击其他网络设备。其常用手法是爆破摄像头密码，利用一些设备默认口令或者常用口令猜解密码。

Mirai 僵尸网络曾发起多次 DDos 攻击，每次影响都非常“闻名”。2016 年 9 月，著名的安全新闻工作者 Brian Krebs 的网站 KrebsOnSecurity.com 受到大规模的 DDoS 攻击，其攻击峰值达到 665Gbps，Brian Krebs 推测此次攻击由 Mirai 僵尸发动。 同样在 2016 年 9 月，Mirai 针对法国网站主机 OVH 的攻击突破 DDoS 攻击记录，其攻击量达到 1.1Tpbs，最大达到 1.5Tpbs。2016 年 10 月，美国域名服务商 Dyn 遭受大规模 DDoS 攻击,其中重要的攻击源确认来自于 Mirai 僵尸。如此数量庞大的物联网设备，其安全问题不容忽视。物联网丰富了我们的生活，同样，也带来不小的麻烦。

根据白帽汇安全研究院对以往摄像头安全事件的总结，现得出部分品牌摄像头的默认密码。

用户名/密码	设备名
admin/123456	ACTi IP Camera
root/anko	ANKO Products DVR
root/pass	Axis IP Camera, et. al
root/vizxv	Dahua Camera（浙江大华摄像头）
root/888888	Dahua DVR（浙江大华）
root/666666	Dahua DVR（浙江大华）
root/7ujMko0vizxv	Dahua IP Camera （浙江大华摄像头）
root/7ujMko0admin	Dahua IP Camera （浙江大华摄像头）
666666/666666	Dahua IP Camera（浙江大华摄像头）
root/dreambox	Dreambox TV receiver
root/juantech	Guangzhou Juan Optical(广州九安光电)
root/xc3511	H.264 - Chinese DVR
root/hi3518	HiSilicon IP Camera
root/klv123	HiSilicon IP Camera
root/klv1234	HiSilicon IP Camera
root/jvbzd	HiSilicon IP Camera
root/admin	IPX-DDK Network Camera
root/system	IQinVision Cameras, et. al
admin/meinsm	Mobotix Network Camera
admin/1111111	Samsung IP Camera
root/xmhdipc	Shenzhen Anran Security Camera(深圳市安冉，雄迈模块)
root/ikwb	Toshiba Network Camera
supervisor/supervisor	VideoIQ
root/<none>	Vivotek IP Camera

表 3-3 部分品牌摄像头的默认密码

3.4 未采用加密协议传输

在对摄像头漏洞进行分析的过程中发现，由于许多摄像头的网页管理界面并没有采用 https 协议进行加密通信，从而导致摄像头极易遭受中间人等一系列信息泄漏和信息篡改的攻击，特别是一些无线远程摄像头（公共场合监控）。

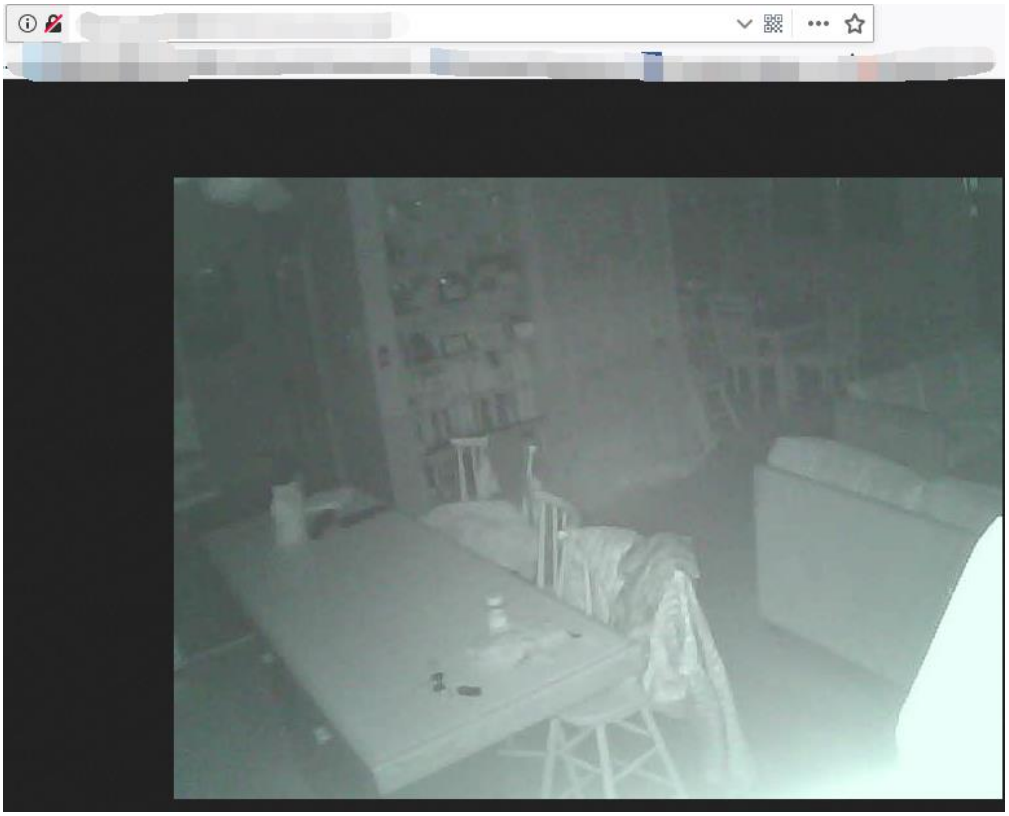

图 3-14 视频的传输没有使用 HTTPS

导致这种结果的原因，一方面是因为部分厂商完全没有考虑传输安全，没有使用 HTTPS 协议；另一方面，部分厂商在使用了 HTTPS 的情况下，位于 80 端口的 HTTP 依然可以使用，从而导致 HTTPS 形同虚设。

3.5 无防范暴力破解的机制

在传统网络安全中，防止暴力破解可以说是所有网站的第一课题。各式各样的验证码以及层出不穷的打码平台每天都在激烈对抗。但对于许多网络上的摄像机来说，登入界面往往不存在任何防范暴力破解的措施，即使有，也是很简单的验证码图片，极易被破解。从而导致黑客可以对注册，找回密码和登入等流程进行无限制的暴力破解，而且整个破解过程用户基本是毫无感知的，更不用说进一步的记录和分析机制。用户往往在暴力攻击的前后都不知晓有摄像头安全事件的发生。

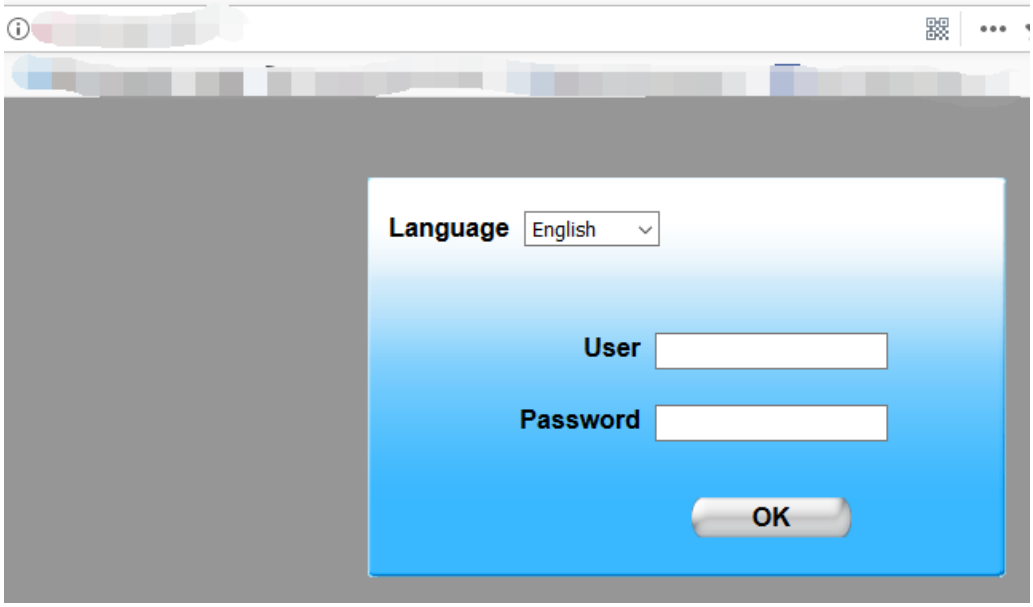

图 3-15 登入界面简陋且无安全措施

3.6 多数设备难对抗重放攻击

研究摄像头的漏洞，往往需要先深入了解某台摄像头的通信机制（通信活动中的身份标识和指令），截取通信流量，然后再套用总结出来的特定标识和参数进行进一步的攻击。大多数的摄像头在面对这类攻击时，没有防重放防御，防御性较差。而且往往同品类摄像头可以利用同样的流量进行控制，形成横向渗透。

图 3-16 互联网中关于重放攻击的搜索结果

3.7 未对客户端进行安全加固

很多品牌的摄像头手机端 APP 并没有进行加固和混淆，轻易就可被黑客逆向破解。黑客在脱离 APP 且未授权的情况下，即可实现对设备内部登入、管理方式控制、甚至是通信时对称加密密钥和所使用的管控接口等的完全操控。

3.8 使用开源代码引入缺陷

一方面，市面上不少摄像头的底层使用的是同一套开源代码。一旦源码出现问题将波及诸多品牌的设备。在 2017 年，一个名为“gSOAP”的摄像头开源代码被发现有一个严重的安全漏洞，黑客可利用这个漏洞实现摄像头的远程操控。经过调查发现，此漏洞波及了 249 种型号的 Axis（Axis 是最大的互联摄像头生产商之一）摄像头。此外，还有其他 34 家公司的产品也受到了影响。这一影响还不包括个人使用源码的情况。

另一方面，某些摄像头厂商自编的代码存在质量问题，容易出现传统网络安

全中诸如验证机制、读写保护以及逻辑漏洞等各类源码问题。

3.9 无安全管理措施

与电脑和手机的软件更新机制不同，摄像头设备因具有在离网状态下可持续稳定使用的特征，其更新和漏洞修复全然依仗于用户的自主操作。而由于用户集中于线下实体店或网络的购买渠道的限制，用户对摄像头厂商的漏洞和更新公布存在严重的信息不对称。设备漏洞更新信息无法有效传达，加之更新存有操作复杂且极具滞后性的特点，使得摄像头设备的远程更新难以实现。而对于某些影响范围极广的漏洞而言，若不能短时间进行迅速修复，那么带来的危害将是无法估量的。

4 摄像头黑色产业分析

4.1 DDOS 攻击

除隐私视频贩售以外，网络黑产业中还流行通过摄像头漏洞植入僵尸程序，发起 DDOS 攻击，进而以有偿提供 DDOS 服务或者勒索的方式从中获利。2016 年 10 月 21 日，美国东海岸网络大规模断网事件就是源于 Mirai 僵尸程序的感染。攻击者通过控制僵尸网络对全球数十万台摄像头设备发起超过 1TB 的攻击流量，从而导致超过半数的美国人无法上网。当时，推特（Twitter）、亚马逊（Amazon）、爱彼迎（Airbnb）均受到严重影响。在 2016 年 9 月，OVH 遭遇了每秒 1TB 的 DDos 攻击。黑客通过入侵数万个 CCTV 摄像头，打造了一个含有 145607 个摄像头的僵尸网络。黑客就是通过这一网络同时向同一个地址发送数据包，很轻松地完成了一场 TB 级别的 DDos 攻击。

白帽汇安全研究院经过对近 3 年与摄像头攻击有关的安全事件整理，得出以下和摄像头有关的攻击事件列表。

时间	事件
2016 年 6 月份	一珠宝店遭受 25000 个摄像头的 DDos 攻击，每秒发起 50000 次垃圾 HTTP 请求
2016 年 9 月份	法国一家服务器托管公司 OVH 遇了前所未有的大型 DDos 攻击，共有 145607 个摄像头参加攻击，峰值流量达到了每秒 1TB
2016 年 10 月份	互联网上的物联网设备(网络摄像头等)构成 Mirai 僵尸网络，发起 DDos 攻击，造成巨大威胁
2016 年 10 月份	大量摄像头 DDos 美国 DNS 服务器，致使美国网络大面积瘫痪
2017 年 3 月份	安全人员发现由超过 5 万台网络摄像头组成的 http81 僵尸网络
2017 年 6 月份	大量摄像头组成的“川普僵尸”物联网僵尸网络通过 HTTP 和 UDP 进行攻击
2018 年二季度	日本出现了一个由 50000 个监控摄像头组成的僵尸网络。

表 4-1 与摄像头有关的攻击事件列表

4.2 挖矿

近几年，加密货币的兴起为黑客透过摄像头非法获利提供了一种“安全”的方式，即挖矿。有别于正常的挖矿，黑客的挖矿是透过僵尸程序的植入，利用他人资源进行挖矿。在此过程中，尽管黑客使用的介质是与电脑芯片性能相差甚远的低性能摄像头 ARM 芯片，但当劫持的摄像头设备达到一定数量后，所获得的收益也是非常可观的。

在今年于西班牙举办的 2018MWC 大会上，捷克网络安全公司 Avast 实际演示了 15000 台小件联网设备 4 天内的“挖矿”过程。结果显示，15000 台小件联网设备可在 4 天内挖掘出价值 1000 美元的加密货币。基于目前智能摄像头使用量的增长曲线和便宜廉价的价格定位，预计未来网络摄像头的数量将远远超过全球电脑的数量。届时，智能摄像头的算力将成为挖矿攻击者争夺的“大蛋糕”。与此同时，网络摄像头完整修复体系的缺失更是为攻击者们提供了一张畅通无阻的“通行证”。品牌和标准的杂乱也为产品的快速修复和挖矿者的追溯提供了难度。

目前可以确定的是，挖矿对于攻击者来说具有匿名性，这就更加难以追查到攻击者，尽管目前的实际攻击案例很少，但在未来可能是一个发展趋势。

4.3 隐私视频售卖

现实生活中，大量隐私视频在当事人并不知情的情况下在网络中传播。这一现象的背后实际上是一条集黑客破解、买卖、偷窥于一体的网络黑产链。黑客入侵摄像头获取到隐私视频（如偷窥视频）后，非法将之出售给从事偷窥和色情等非法交易的组织或个人。这些组织或个人在获得隐私视频后将之提供给非法博彩或成人用品的电商平台或钓鱼网站导流使用，从而从中谋得经济利益。而此类隐私视频的曝光将给视频当事人的生活埋下极大的隐患。

图 4-1 QQ 群搜索摄像头黑产结果

图 4-2 QQ 群搜索摄像头黑产结果

图 4-3 QQ 群搜索摄像头黑产结果

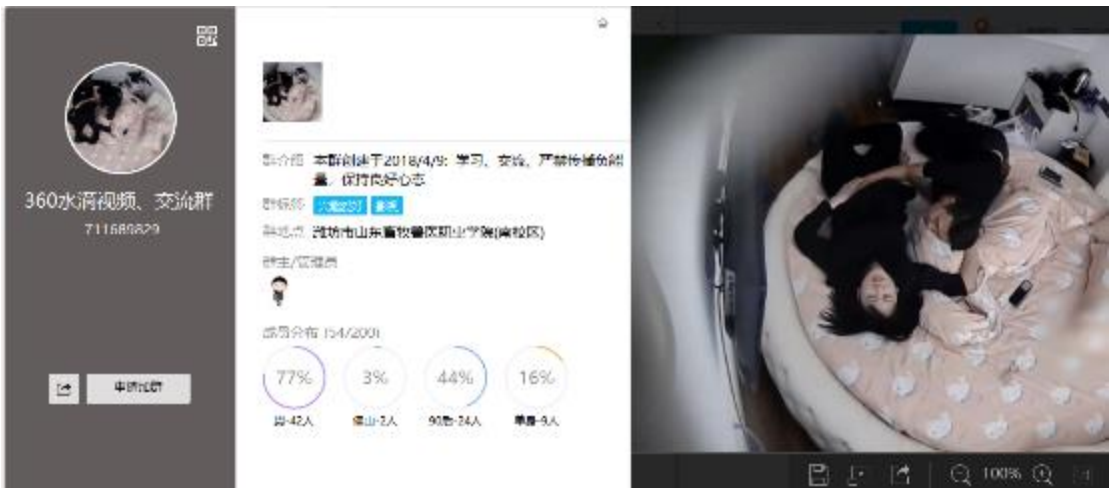

图 4-4 众多 qq 群都涉及这个黑色产业

也就是说，随着网络黑产链从业者的入侵，用户诸如躺在床上玩手机等日常生活场景将很有可能通过这条产业链完全暴露给某些人群，以满足其特殊的需求。攻击者们通常采用建立网络群聊的方式进行非法视频资源的售卖。他们多以群聊为平台，通过截图、钓鱼、诱惑的方式吸引特殊人群上钩。随后，便可交流进行私人家用摄像头资源的贩卖。至此，用户的隐私就被当作“商品”在网络公开售卖。

实况摄像头		价格
家庭ID（有看头）	12个	98元
酒店ID360水滴账号	15台	288元
ID剪辑视频		价格
家庭精彩剪辑	60部	88元
宾馆精彩剪辑	60部	138元
软件类		价格
正版守望者/云视通（pc版）		300元
色情直播软件（安卓+ios）		128元
看片软件（安卓）		88元

以前均有货。不单卖不试看买多可议价。诚信为本

图 4-5 网络中售卖摄像头资源的案例

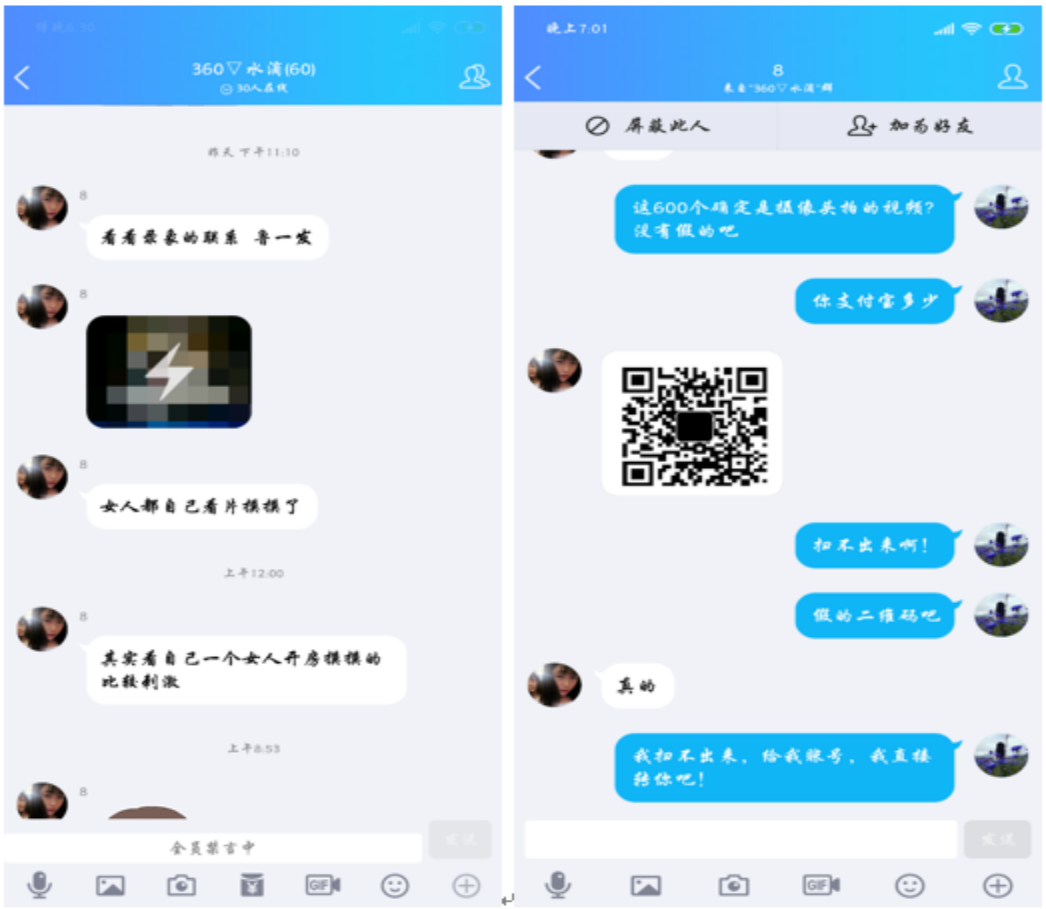

图 4-6 网络中售卖摄像头资源的案例

除诈骗外，还有出售摄像头资源卖家，600 个视频售价 200 人民币，用户的隐私就被非法人员在网络公开售卖。

图 4-7 黑产利用工具界面

图 4-8 黑产严重“高质量”资源

此外，部分黑产人员还通过出售 APP 的方式进行售卖操作。有特殊需要的人群只需通过 APP 账号充值的方式，就可获取在线观看隐私视频的权限。充值金额越高，所获得的摄像头 IP 地址“质量”就越高。这里所谓的“高质量”IP 就是家庭卧室的摄像头。

5 摄像头安全对策

若要从根本解决摄像头安全问题，需以安全管理和安全技术相结合来解决专网视频监控的安全问题。对于互联网来讲也可同样采用相同的思路。加强安全管理措施，同时辅以技术手段提高效率，快速解决安全问题。

5.1 安全管理

5.1.1 安全标准

安全标准是开展摄像头安全建设工作的基础和行为指南。2017 年公安部发布了 GB35114-2017 《公共安全摄像头联网信息安全技术要求》，并宣布于 2018 年 11 月 1 日正式实施。该标准是由公安部提出、全国安全防范报警系统标准化技

术委员会(SAC/TC100)归口、经国家质量监督检验检疫总局和国家标准化管理委员会批准发布的国家安全标准。其对公共安全领域摄像头联网视频信息以及控制信令信息安全保护的技术要求进行了详细规定,适用于公共安全领域摄像头系统的信息安全方案设计、系统检测及与之相关的设备研发与检测。

但此标准仅对公共摄像头的安全进行了规范，却依旧并未涉及摄像头厂商和家庭摄像头的安全。此安全标准的局限与庞大的摄像头应用相比，无疑是存有较大漏洞的。因此，强化摄像头生产标准的规范、增强生产标准的评审、监测等防护测试、完善家庭摄像头安全标准体系等应当成为摄像头安全寻求突破性建设的下一步规划。与此同时，相关部门在标准出台后，应积极加快安全标准的实施，尽可能快地实现摄像头安全的高效提升。

5.1.2 统一化安全管理

摄像头的最大风险在于没有有效的管理手段、资产管理混乱等。针对这种情况，采用统一的集中化管理，可避免专业性差、管理混乱、没有解决问题的技术带来的风险。

统一化其中一部分是摄像头的网络资产管理，另外一部分为安全维护的管理。通过接入专网，配合网络空间探测技术，对资产进行统一管理。通过对摄像头产品漏洞进行监控，出现最新漏洞也可以快速反应，先于黑客发现漏洞，并在此之前修复。

5.2 安全技术

目前摄像头的安全研究已经为越来越多的安全厂商所重视。近两年的数据显示，摄像头漏洞补丁的数量呈现出稳步增长的趋势。这一趋势对于摄像头设备安全的提升工作无疑是一个良好的开始。

支撑技术方面，白帽汇安全研究院建议相关部门和企业用户可充分利用网络空间测绘技术以及产品（如网探 D01）的功能对公共安全摄像头和企业内部摄像头进行安全巡检，尽量使摄像头的安全隐患处理做到早预防、早发现、早修复，切实地提高关键信息基础设施和企业内部的安全管理。网络空间测绘技术在解决

公共摄像头和商用摄像头管理混乱问题、规范资产管理和安全漏洞发现预警方面，都能起到及时预警、高效应对和降低风险危害的作用，对于摄像头安全的提升有着明显的助益。

5.2.1 安全厂商

说到网络安全就不得不提及漏洞，而漏洞修复是解决网络安全问题最核心的内容。随着安全厂商和安全从业人员的加入和队伍的不断壮大，越来越多的摄像头设备漏洞逐步被发现。越来越多的安全厂商结合推行的安全标准、安全检查，积极地加入到漏洞修复工作中，整个行业的安全系数不断提升。目前中国有数十万的白帽子，他们将会是一股推动摄像头安全实现变革式发展突破的攻坚力量。国家和摄像头制造商们应当充分调动起这股力量的积极性和参与性，继而为整个行业安全系数的提升提供助力。

除漏洞研究外，另一重要的及时摄像头的安全防御部分。摄像头类设备因体积小，计算和存储能力较之计算机都有较大差异。因此诸如互联网领域中的防火墙、防毒产品等安全防御技术的研发将成为提升摄像头安全系数亟待攻克的难题之一。此时，致力研发全防御技术的安全厂商将成为保证摄像头源头安全的“卫士”。安全厂商通过全芯片、物联网防火墙等的研究，从防御层面拦截漏洞利用和攻击者，实现摄像头设备初始安全环境的净化。

5.2.2 摄像头制造商

除针对摄像头的设备的特点进行针对性防护外，还需要在整个业务系统从研发、上线、报废的生命周期内实施生命周期的安全管理。确保安全管理体系可以覆盖业务节点，实现及时发现每一环节中引入的漏洞等安全问题。

方向	内容	说明
开发安全	开发环境	制造商开发环境保障安全、构建企业自身安全
	源代码安全	进行漏洞审计，确保开发上线之前系统代码层面安全。
	模糊测试	对设备进行模糊测试，以进行黑盒方面的安全测试。
网络安全	身份认证	使用安全的认证方式，加强认证权限，设置合理的身份认证。
安全传输	通信安全	使用 SSL 加密对网络数据进行安全传输
安全规范	安全规范	产品说明简历对用户的安全指导与建议，引导用户对设备进行安全配置。

表 5-1 摄像头安全体系

安全厂商也可运用网络空间测绘技术对自己已经售卖出去的摄像头进行盘查，让摄像头厂商更容易掌握摄像头的归处以及暴露情况，在发现问题时及时通知用户。

5.2.3 企业或机构用户

就目前企业或机构用户而言，其在摄像头设备的使用过程中，存在着管理基数庞大且管理混乱、人员更换导致安全管理缺失等安全问题。基于此，企业或机构用户应当根据企业或机构的实际情况，利用网络空间测绘技术对内部的摄像头设备进行排查，盘点出网络资产的实际情况，继而在对相关设备和资产进行全面检查。针对相关问题，采取对应的安全防护措施，尽可能地避免损失的发生。

5.2.4 个人用户

对于个人用户而言，应注重自身摄像头设备和网络安全意识的培养，提升安全防范意识，养成包括为摄像头设备设置安全密码等在内的良好安全习惯，进而避免给生活和工作带来不必要的麻烦。

6 总结

摄像头已经无处不在，充斥整个社会。摄像头安全已经成为当下必须要面对和解决的难点。本报告基于视频专网的安全现状到互联网摄像头安全现状，就摄像头安全问题、安全风险及黑色产业情况进行研究，以解决安全困局为目的，通过统一化资产管理、自动检查、监控点位等管理手段对视频专网和网络互联网进行充分管理。通过管理推动落实安全技术，增强摄像头安全行业水平。

基于网络空间测绘技术和 FOFA 系统，对全网摄像头的开放情况进行了相关统计与分析，着重揭示了全球和中国地区摄像头的对外暴露情况。经由摄像头设备的安全漏洞，攻击者可通过漏洞入侵、植入僵尸发起 DDOS 攻击、挖矿等方式，对摄像头设备信息和数据进行隐私贩卖或恶意篡改和控制，严重威胁着企业、国家和民众的网络甚至人身安全。随摄像头漏洞挖掘利用而增长的是摄像头安全漏洞情况的加剧恶化。加之安全防护体系的薄弱现状，摄像头安全问题的解决势在必行。

摄像头设备应用的特点决定摄像头的安全问题应将国家、企业和个人都纳入在内。发动国家、企业和群众的力量，从标准制定、资产排查、风险监测、漏洞修复等多个方面，提高摄像头的安全性，建立和完善摄像头网络安全防护体系是全面推进摄像头安全生态优化的有效思路。而网络空间测绘系统将成为此过程中的重要技术力量和推动摄像头安全发展的技术突破口。

最后，本报告所使用的暴露情况统计数据主要来源于 FOFA 系统，漏洞统计则主要以 CNNVD 和 CVE 两大机构的统计数据为依据。虽然已通过逐一确认的方式尽可能地确保数据准确性，但由于样本的局限性，上述数据尚不具备全面覆盖性。然而本报告着重于通过系统数据统计揭示摄像头的暴露情况、安全漏洞情况和黑产情况等，故少量遗漏并不影响报告结论论述。

附录 1 北京华顺信安科技有限公司

北京华顺信安科技有限公司(www.huashunxinan.net)是一家专注于网络空间测绘、安全大数据的互联网安全公司。作为网络空间测绘的领跑者，主要从事网络空间测绘分析、网络信息安全领域的技术和产品研发工作，为国家网络安全提供技术支持，为政企用户提供顶级网络信息安全防护服务。

公司旗下“白帽汇安全研究院”，成立于 2015 年 7 月，在网络空间测绘技术方面居于全球领先水平。研究院在网络安全领域拥有多项知识产权，现已成为中国互联网网络安全威胁治理联盟的首批成员单位及国家信息安全漏洞库二级技术支撑单位。2016 年受国家信息技术安全研究中心委托，提供银行业伪基站钓鱼网站诈骗数据。

网络空间测绘作为网络安全的根基，其重要性不言而喻，公司经过 3 年多的努力和沉淀，已经具备了在行业内首屈一指的实力。

FOFA-网络空间安全搜索引擎（fofa.so）

网络空间资产检索系统（FOFA）是世界上数据覆盖最完整的 IT 设备搜索引擎，拥有全球联网 IT 设备最全 DNA 信息。探索全球互联网的资产信息，进行资产及漏洞影响范围分析、应用分布统计、应用流行度态势感知等。

FOFA 是白帽汇推出的一款网络空间搜索引擎（共有 7.4 亿服务数据、5.5 亿网站、7 千多条查询规则），它通过进行网络空间测绘，能够帮助研究人员或者企业迅速进行网络资产匹配，例如进行漏洞影响范围分析、应用分布统计、应用流行度排名统计等。

FOFA-网络空间安全搜索引擎

FOEYE-网络空间检索系统

FOEYE-网络空间测绘系统为 CIO（首席信息官）服务，超越 ITSM 产品，实时登记企业网络中入网设备清单，包括设备型号、中间件、运行软件等组件，提升硬件利用率，降低设备空置率。**全面、快速、精准的资产发现，可实时消除高达 40%的盲点资产并实时检测潜在威胁。**智能标记**风险资产**，通过 FOFA PRO 客户端漏洞库平台库，轻松自如面对未来的“永恒之蓝”漏洞，降低网络安全风险。

FOCII-关键信息基础设施测绘系统（focii.cn）

基于互联网侧关基设施普查，通过主动和被动方式全面快速收集资产。POC 漏洞专扫，为企业快速定位风险资产，并分析验证、漏洞影响范围统计等安全防

护等，帮助企业全面快速地搜集资产并开展安全管控。

NOSEC-安全讯息平台（nosec.org）

NOSEC 安全讯息平台提供快速、专业、深入、全面的安全资讯平台，结合安全大数据为用户提供威胁情报、安全动态、漏洞预警、专题报告、技术分析、安全工具等行业最新的安全讯息。

附录 2 参考

[1] FOFA Pro-网络空间安全搜索引擎，网络空间搜索引擎，网络空间测绘，安全态势感知 https://fofa.so
[2] GB35114-2017 国家强制标准实施 人民公安报整版专题报道阐述其重大意义 http://security.asmag.com.cn/news/201811/96411.html
[3] 数十万网络摄像头存漏洞：黑客可远程入侵 http://news.mydrivers.com/1/595/595362.htm
[4] 视频监控出现新漏洞：黑客可以让监控摄像头失灵 https://tech.sina.com.cn/it/2018-09-18/doc-ifxeuwwr5433052.shtml
[5] 视频监控出现新漏洞：黑客可以让监控摄像头失灵 http://www.sohu.com/a/254494636_100191017
[6] Axis 摄像头存在安全缺陷，三个漏洞即可接管 http://www.freebuf.com/news/175224.html
[7] 智能摄像头安全漏洞太多，小米 360 均上榜，你家中招了吗？ https://baijiahao.baidu.com/s?id=1570598887635349&wfr=spider&for=pc
[8] 漏洞百出——360 报告揭露智能家庭摄像头行业安全乱象 http://science.china.com.cn/2016-11/17/content_9164620.htm
[9] 摄像头存漏洞 数百万物联网设备面临被黑风险 http://www.techweb.com.cn/world/2017-07-20/2560344.shtml
[10]智能摄像头质检八成不安全 易被黑客利用 http://finance.huanqiu.com/chuangr/chuangtou/2017-06/10896577.html
[11]摄像头遭入侵，除了泄漏隐私，还可能引发 DDoS 攻击威胁！ http://www.sohu.com/a/158402727_642860
[12]摄像头搞瘫美国互联网的背后：智能设备漏洞泛滥 https://www.csdn.net/article/a/2016-04-19/4549
[13]物联网时代网络摄像头和 DNS 不得不说的故事 http://security.asmag.com.cn/tech/201702/75931.html
[14]史上最烂挖矿机：黑客用监控摄像头 DVR 挖比特币 http://www.wanbizu.com/news/201409282799.html
[15]从青果直播用户隐私看摄像头安全问题，千万摄像头暴露公网 https://zhuanlan.zhihu.com/p/45415948
[16]谈谈物联网与摄像头安全 https://cloud.tencent.com/developer/article/1040088
[17]手机安全性解决了！家庭摄像头为什么就不行？ http://www.sohu.com/a/194864721_624619
[18]全球有多少摄像头你知道吗？这份报告告诉你 http://www.afzhan.com/news/detail/58574.html
[19]自家监控成直播现场！小摄像头背后的这些隐患要注意了 http://www.xinhuanet.com/politics/2017-06/20/c_1121178995.htm
[20]互联网的眼睛 - 网络摄像头 http://www.zerokeeper.com/web-security/internet-eyes-webcam.html
[21]中国公司拟对摄像头召回：被指引发全美网络瘫痪

http://news.mydrivers.com/1/504/504667.htm
[22]从易牙烹子泄密看网络摄像头漏洞的危害
https://t.cj.sina.com.cn/articles/view/6459181845/180ff4b1500100bfs7
[23]【物联网安全】系列之一：隐藏在摄像头下的罪恶 http://blog.nsfocus.net/iot-security-webcam/
[24]城市监控摄像头系统普遍存在不安全性 https://www.kaspersky.com.cn/blog/urban-surveillance-camera-systems-lacking-security/3105/
[25]【漏洞预警】雄迈云服务器内置硬编码账户漏洞（CVE-2018-17919）
https://nosec.org/home/detail/1893.html
[26]【漏洞预警】NUUO 摄像头最新高危漏洞预警(CVE-2018-1149)
https://nosec.org/home/detail/1828.html
[27]【漏洞预警】数十万酷视网络摄像头存在高危风险，可导致视频泄漏、被植入僵尸网络等风险
https://nosec.org/home/detail/1722.html
[28]【漏洞预警】AXIS 大量摄像头产品多个连环漏洞利用，影响严重
https://nosec.org/home/detail/1675.html
[29]Sony IPELA E 系列网络摄像头远程命令执行漏洞预警
http://blog.knownsec.com/2018/08/sony-ipela-e-%E7%B3%BB%E5%88%97%E7%BD%91%E7%BB%9C%E6%91%84%E5%83%8F%E5%A4%B4%E8%BF%9C%E7%A8%8B%E5%91%BD%E4%BB%A4%E6%89%A7%E8%A1%8C%E6%BC%8F%E6%B4%9E%E9%A2%84%E8%AD%A6/
[30]【国际资讯】我国网络摄像机制造商 Foscam 被爆存在 18 个安全漏洞
https://www.anquanke.com/post/id/86235
[31]三星智能监控摄像头被爆远程代码执行漏洞（含 POC）
https://www.anquanke.com/post/id/84396
[32]D-Link 云摄像头超过 120 款产品存在漏洞，约 40 万台设备受影响
https://www.freebuf.com/news/108870.html
[33]某 CCTV 摄像头漏洞分析
http://www.vuln.cn/6939
[34]干货|盘点，近三年来物联网产业相关国家政策
https://www.sohu.com/a/168282440_221974
[35]网络监控 2013：IP Camera 民用市场暴增
http://news.cps.com.cn/article/201312/751601.html
[36]2017 年中国视频监控行业市场规模与前景预测
https://www.qianzhan.com/analyst/detail/220/171206-1a8c4bbc.html