



## IoT安全的To B与To C

王滨 海康威视CSO





## IoT设备包括哪些？

FIIT 2019

工业智能机器人  
家用路由器  
摄像头  
心脏起搏器  
自动驾驶汽车  
智能家居  
心脏起搏器  
手环  
各种传感器  
智能音箱  
智能窗帘



## 公众眼中的IoT安全



## 央视曝光大量家庭摄像头遭破解，防止隐私泄露做到这几点很重要

**FULL**

众所周知,随着智能电子设备的快速发展,一些新兴的高科技产品逐渐进入普通家庭的生活,例如家用摄像头,因为具有远程监控的优点,很多家庭都安装了智能摄像头,即使出门在外,也可以用手机随时查看家里的情况。这对于看护老人、小孩、宠物以及防止家

细思极恐，当你的车辆被黑客远程控制

2008-09-29 11:43:27

今年11.5期间通过一保制度，提前排查治理安全隐患，防止生产安全事故发生。

4月15日，有网友在知乎上发帖称，自己于4月14日在北京市朝阳区某小区，看到一名男子在小区内散步，该男子穿着黑色运动服，戴着黑色口罩，手里拿着一个黑色的包。该男子在小区内散步时，突然从包里拿出一个黑色的袋子，将袋子打开，里面装满了现金。该男子将现金放在地上，然后转身离开。该网友称，自己当时正在小区内散步，看到这一幕后，立即上前查看，发现现金是100元人民币。该网友称，自己当时感到非常震惊，不知道该怎么办。该网友称，自己当时感到非常震惊，不知道该怎么办。该网友称，自己当时感到非常震惊，不知道该怎么办。

[搜狐健康](#) > [健康产业](#) > [健康新闻](#)

## 黑客控制心脏起搏器杀人？安全专家称可以实现

此堂 我輩這間每戶人家都

2023年10月25日 来源：人民网

[返回首页](#)
[网站地图](#)
[联系我们](#)

原標題：「黑心炒粉店」被揭開黑幕 人手天厚 安全衛生難以保障

从深圳到台北再到香港（记者 蓝彬 陈健）最近两岸媒体，高雄和基隆的制心引起热议，这似乎让人产生联想。在遭受人民网采访时表示，在特定的场景中，剧本

中国网·中国

滚动

女孩跑步时戴运动手环 全程被监测 盘点曾被偷窥的尴尬场面(图)

2005-11-17 11:50

来源：本局解作图：李昭平 | T

地址：上海南京路100号

亚马逊旗下智能音箱存在漏洞可被变成黑客的监控工具

2010年10月22日 星期五 10:28:27 PM

正版软件商城

此項調整係上列PACCO對策。

4002

1000

【附註】大立資訊公司基本盤十分穩固，主要係已穩佔若干人工智慧辨識裝置與APP開發等一連串技術與專利，特別是其專為「智慧辨識系統」所開發之技術，甚至為美國政府所採買，每年可賺取美金逾百萬元之利潤，因此該公司之股價表現亦十分穩固，特別是在今年年初至年中間，更曾一度漲至最高點。





# 安全研究人员眼中的IoT安全

IT 2019

搜狐 > 科技 > 正文

落纸生花创意  
折纸

168 30万  
点赞 评论

查看TA的相册>

## 黑客只要三步就能操作你的网络摄像头！

2017-01-03 16:27

写在前面的话：  
我并不是想吓唬大家，  
现在我已经和  
后面这些就是  
放假了。  
操作如下：  
打开局域网扫描工具  
以我公司的摄像头为例  
首先我查到了  
至于如何搞定  
其实我们每  
全球几百万摄像头在  
几百万！！  
中国地区的也有几十  
我们随便找一个IP地址  
输入默认的账号密码，最少百分之80的是没改密码的！

1 2 3 4 5 6

ZoomEye

搜索范围  
公网IP  
内网IP  
Port

- 弱口令
- 暴露在互联网上
- 漏洞

[http://www.sohu.com/a/123283355\\_266823](http://www.sohu.com/a/123283355_266823)



## IoT安全的ToB&ToC

IFT 2019

ToB : 弱口令、漏洞、暴露在互联网上

ToC : 弱口令、漏洞



ToC—设备可以不暴露在互联网上

FT 2019





## ToB—设备大量暴露在互联网上

FT 2019

- 本身为了应用的需要暴露在互联网上
- 设置不当导致设备暴露在互联网上





## IoT设备安全永远的痛--弱口令

IT 2019

用户：安全意识淡薄，亟待提高

厂商：早先的产品存在密码硬编码/未使用更加健全的口令机制

国家信息安全标准委员会（TC260）

《信息安全技术-智能联网设备口令保护指南》





# IoT设备安全无法回避的问题—漏洞

IT 2019





## ToC安全该怎么做？

FT 2019





## ToB安全该怎么做？

IT 2019

- 设备需要开放多种端口
- 用户安全意识普遍不高
- 系统网络环境复杂多样
- 纵深防御很难有效实施
- 历史累积问题堆积如山



- 厂商提供更高产品安全要求
- 为用户提供轻管理的安全防护方案



## IoT设备漏洞的几点呼吁

IT 2019

- 目前业界遵循的90天的漏洞披露策略对于无有效升级途径的物联网设备并不适用；
- POC的检测更推荐采用版本检测的方式；
- 用户设置周期性固件更新计划任务，弱口令一定要避免；
- 厂商加强设备的安全设计、开发、测试和应急响应；
- 行业主管机构必须要有强制的检查和通报机制

REEBUF | FIT

THANKS