

原文：<https://embedi.com/blog/reflecting-upon-owasp-top-10-iot-vulnerabilities/>

众所周知，嵌入式设备在安全机制和服务的实现方面还面临许多问题，鉴于此，OWASP物联网项目针对智能设备**最常见IoT漏洞**进行了详细的分类。

为了帮助读者加深理解，我们为每种类型的漏洞提供了现实中的例子。我们希望智能设备用户在阅读本文后，能够全面意识到每天会面临哪些威胁。读者会发现，为每种漏洞








当然，某些实例其实属于多种漏洞类别，因为它们同时含有不同的安全漏洞，这进一步说明物联网设备的安全性的确让人堪忧。

注意：OWASP在漏洞类别中使用了一些缩略词，其含义如下所示：

- “A”表示应用程序
- “I”表示物联网
- “M”表示移动设备

I1 不安全的Web接口

一般情况下，攻击者首先会在智能设备的Web接口中寻找XSS、CSRF和SQLi漏洞。此外，这些接口中还经常出现“默认用户名和密码”和“缺乏帐户锁定机制”之类的漏洞。

设备类型	设备名称	CWE	安全影响
	Heatmiser恒温器	CWE-598：通过GET请求中的查询字符串泄露信息	攻击者可以访问设备的所有设置，进而根据攻击者
	工业无线接入点Moxa AP	CWE-79：网页生成过程中没有对输入进行严格过滤	攻击者可以获取设备上的会话，并且该会话永不
	AXIS相机	CWE-20：输入验证不当	攻击者能够以root权限编辑操作系统中的任意文件
	Belkin智能家居产品	CWE-79：网页生成过程中没有对输入进行严格过滤	攻击者可以获取设备上的会话，并且该会话永不
	路由器 D-Link DIR-300	CWE-352：跨站请求伪造（CSRF）	攻击者可以修改管理员密码并获得root权限。
	AVTECH网络摄像头、NVR、DVR	CWE-352：跨站请求伪造（CSRF）	攻击者可以通过CSRF修改设备的所有设置，如用
	AGFEO智能家居ES 5xx/6xx	CWE-79：网页生成过程中没有对输入进行严格过滤	攻击者可以获取设备上的会话，并且该会话永不



设备名称

Loxone智能家居

CWE-79：网页生成过程中没有对输入进行严格过滤，通过设备本地漏洞的命令来控制设备的所有



交换机TP-Link TL-SG108E

CWE-79：网页生成过程中没有对输入进行严格过滤，在设备本地漏洞存储型XSS代码，进而使



Hanbanggaoke网络摄像头

CWE-650：信任服务器端的HTTP权限方攻击者可以修改管理员密码并获得root权限。



路由器Netgear

CWE-601：URL重定向至不可信站点（Open Redirect漏洞）  
互联网上的任何人都可以利用Cockup来控制该路

## I2 认证/授权漏洞

通常情况下，如果存在这种类型的漏洞，则意味着攻击者可以通过用户的弱密码、密码恢复机制的缺陷以及双因子身份验证机制的缺失来控制智能设备。

设备类型	设备名称	CWE	安全影响
	DV摄像机 Mvpower	CWE-521：弱密码以及CWE-284：访问控制不当	攻击者可以访问DVR的设置，因为登录名和
	DBPOWER U818A WIFI 四轴无人机	CWE-276：不恰当的默认权限	攻击者可以从设备读取文件，如图像和视频文件。
	iSmartAlarm	CWE-287：不恰当的身份验证	攻击者可以向报警装置发送命令，控制报警装置的
	DbiTek GoIP	CWE-598：通过GET请求中的查询字符串泄露信息	攻击者可以通过向GoIP发送命令来修改其配置，比
	Nuuo NVR（网络摄像机）和Netgear	CWE-259：使用硬编码密码	攻击者可以获得root权限，并使用该设备修改外部
	Sony IPELA Engine网络摄像头	CWE-287：不恰当的身份验证	攻击者可以通过摄像头发送被操纵的图像/视频，让
	Western Digital My Cloud	CWE-287：不恰当的身份验证	攻击者可以完全控制设备。



LG真空吸尘器

CWE-287：不恰当的身份验证

攻击者可以远程激活并访问真空吸尘器的实时视频。



Eminent EM6220相机

CWE-312：以明文形式存储敏感信息

攻击者可以获取相机的root权限并监视相机用户。



LIXIL Satis卫生间

CWE-259：使用硬编码的密码

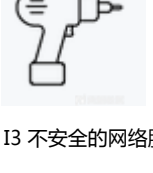
攻击者可能会导致设备突然打开/关闭马桶盖，激活摄像头并发送通知。



机载娱乐系统

CWE-287：不恰当的身份验证

攻击者可以控制向乘客发送通知的方式，如发送虚假信息。



燃料型钻孔机

CWE-259：使用硬编码密码

攻击者可以获取root访问权限并修改钻孔机的设置。

I3 不安全的网络服务

这里主要的问题是“开放了不必要的端口”，“通过UPnP向互联网暴露端口”以及“易受DoS攻击的网络服务”。另外，未禁用的telnet也可能被用作攻击向量。

设备类型	设备名称	CWE	安全影响
 <div>医疗急救设备</div>	智能按摩器	CWE-284：访问控制不当	攻击者可以改变按摩器的参数，这会导致相当痛苦。
 <div>医疗急救设备</div>	植入式心脏设备	CWE-284：访问控制不当	攻击者可以修改植入设备的编程命令，从而导致电击。
 <div>安防网络设备</div>	Hikvision Wi-Fi网络摄像头	CWE-284：访问控制不当	攻击者可以远程利用或禁用摄像头。
 <div>安防网络设备</div>	Foscam C1室内高清摄像机	CWE-120：缓冲区复制过程中没有检查输入大小，导致缓冲区溢出。在摄像机上运行通用缓冲区溢出漏洞可能导致用户个人信息在公共网络上公开。	
 <div>玩具设备</div>	玩具Furby	CWE-284：访问控制不当	攻击者可以修改固件并使用Furby来监视儿童。
 <div>玩具设备</div>	玩具My Friend Cayla	CWE-284：访问控制不当	攻击者可以收集用户的信息并实施监控。
 <div>智能家居设备</div>	iSmartAlarm	CWE-20：输入验证不当	攻击者可以冻结SmartAlarm，使其停止响应。



iSPY Camera Tank

CWE-284：访问控制不当

攻击者可以以匿名用户的身份登录设备，并可以访

I4 缺乏传输加密/完整性验证

这里的问题主要集中在敏感信息以明文形式传递，SSL/TLS不可用或配置不当，或使用专有加密协议方面。含有这类漏洞的设备容易受到MiTM攻击。

设备类型	设备名称	CWE	安全影响
	Owlet Wi-Fi婴儿心脏监护仪	CWE-201：通过发送数据泄露信息	攻击者可以监视婴儿及其父母。
	三星冰箱	CWE-300：通过非端点访问通信信道（中间人攻击漏洞）	攻击者可以窃取用户的Google凭据。
	大众汽车	CWE CATEGORY：加密问题	攻击者可以克隆遥控器并获得未经授权的汽车访问。
	HS-110智能插座	CWE-201：通过发送数据泄露信息	攻击者可以控制插头的状态，如关闭其LED。
	Loxone智能家居	CWE-201：通过发送数据泄露信息	攻击者可以控制智能家庭系统中的每台设备并窃取
	三星智能电视	CWE-200：信息泄露	攻击者可以监控无线网络并进行暴力破解，以恢复
	路由器Dlink 850L	CWE-319：以明文形式传输的敏感信息	攻击者可以远程控制设备。
	Skaterboards Boosted, Revo, E-Go	CWE-300：通过非端点访问通信信道（中间人攻击漏洞）	攻击者可以窃取设备发送各种命令来指挥它。
	LIFX智能LED灯泡	CWE-327：使用可破解或危险的加密算法	攻击者可以捕获并解密流量，包括网络配置等。
	DJI Spark无人机	CWE-327：使用可破解或危险的加密算法	攻击者可以访问设备的设置。

I5 隐私问题

OWASP将该漏洞定义为“收集的个人信息过多”，“收集的信息没有得到适当的保护”，以及“最终用户无权决定允许收集哪类数据”。

设备类型	设备名称	CWE	安全影响
	Gator 2 smartwatch	CWE-359：泄露隐私信息（侵犯隐私）	攻击者可以访问包含软件版本、IMEI、时间、定位
	路由器D-Link DIR-600和DIR-300	CWE-200：信息泄露	攻击者可以读取设备的敏感信息，或使其成为僵尸
	三星智能电视	CWE-200：信息泄露	攻击者可以找到用于录音的二进制文件。
	家庭安全摄像头	CWE-359：泄露隐私信息（侵犯隐私）	用户的私人照片可能被攻击者盗取并公布到互联网
	智能成人玩具We-Vibe	CWE-359：泄露隐私信息（侵犯隐私）	攻击者可以获取设备温度和振动强度等信息。
	iBaby M6婴儿监视器	CWE-359：泄露隐私信息（侵犯隐私）	攻击者可以查看用户的信息，包括视频录像等。







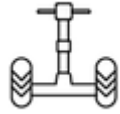
I6 不安全的云接口

通常情况下，这种类型的漏洞意味着，只要攻击者能够访问Internet，就可以获取私人数据。一方面，用于保护存储在云中的私人数据的加密算法的加密强度通常很弱；另一方面，

设备类型	设备名称	CWE	安全影响
	Seagate Personal Cloud Home Media Storage	CWE-598：通过GET请求中的查询字符串注入信息	攻击者可以注入任意系统命令并窃取用户的私人数据
	iCloud	CWE-307：身份验证尝试次数限制不当	攻击者可以访问用户存储在云中的私人照片。
	Vtech gadgets	CWE-359：泄露隐私信息（侵犯隐私）	攻击者可以访问用户的信息进而实施勒索。
	Western Digital My Cloud	CWE-287：不恰当的身份验证	攻击者可以完全控制设备。
	路由器Dlink 850L	CWE-319：以明文形式传输的敏感信息	攻击者可以获得对设备的完全控制权。

I7 不安全移动设备接口

这里的主要问题是“弱密码”，“缺乏双因子认证”和“无帐户锁定机制”。这种类型的漏洞常见于通过智能手机管理的物联网设备。

设备类型	设备名称	CWE	安全影响
	亚马逊智能锁	CWE-284：访问控制不当	攻击者可以打开门锁。
	智能成人玩具Vibratissimo	CWE-359：泄露隐私信息（侵犯隐私）&CWE-284：访问控制不当	攻击者可以访问用户的身份数据，包括清晰的图像。
	智能网络摄像头	CWE-312：以明文形式存储敏感信息	攻击者可以像用户那样使用该应用程序——例如，
	智能插座	CWE-319：以明文形式传输的敏感信息	攻击者可以卸载已经安装的软件，并于原软件所在
	运动手环（Fitbit、苹果、小米、Garmin、三星等）	CWE-319：以明文形式传输的敏感信息	攻击者可以监视运动手环的用户。
	Wink和Insteon智能家居系统	CWE-613：会话失效时间不当	攻击者可以窃取用户的证书并使用已经连接的设备
	Segway Ninebot	CWE-359：泄露隐私信息（侵犯隐私）	攻击者可以访问用户的地理位置。

18 安全可配置性不足

这个漏洞的本质在于，由于用户无法管理或应用安全机制，导致安全机制无法对设备充分发挥作用。有时，用户根本不知道这些机制的存在，这样为设备配置安全设置就成为

设备类型	设备名称	CWE	安全影响
	ADSL设备ZTE ZXDSL	CWE-15：允许外部人员控制系统或进行配置	攻击者可以重置设备的配置。
	毛绒玩具	CWE-521：弱密码	儿童及其父母的录音的存储机制不够安全，这使得
	Canon打印机	CWE-269：权限管理不当&CWE-295：证书管理不当	攻击者可以访问保护不当的设备并更新其固件。
	Parrot AR.Drone 2.0	CWE-285：授权不当	攻击者可以通过移动应用程序无线控制无人机。



Smart Nest Thermostat

CWE-269：权限管理不当

未经授权的攻击者可以访问Nest帐户。

I9 不安全的软件/固件

攻击者能够安装任意固件（无论是官方还是自定义的固件），因为系统没有进行相应的完整性或真实性检查。此外，攻击者还可以通过无线通信完全接管设备。

设备类型	设备名称	CWE	安全影响
	路由器D-Link DIR8xx	CWE-295：证书验证不当	攻击者可以更新路由器的固件，使设备变成僵尸网络。
	GeoVision公司的设备	CWE-295：证书验证不	攻击者可以更新固件并完全接管设备。
	ikettle智能咖啡机	CWE-15：允许外部人员控制系统或进行配置	攻击者可以完全控制设备，例如，打开设备并使其过热。
	Billion路由器7700NR4	CWE-798：使用硬编码的证书	攻击者可以完全控制设备。
	iSmartAlarm	CWE-295：证书验证不当	攻击者可以获取用户的密码或个人数据。
	路由器Dlink 850L	CWE-798：使用硬编码的证书	攻击者可以完全控制设备。

I10 糟糕的物理安全

只要拆开智能设备，攻击者就能找到其MCU、外部存储器等。此外，通过JTAG或其他连接器（UART、I2C、SPI），攻击者还可以对固件或外部存储器进行相应的读写操作。

设备类型	设备名称	CWE	安全影响
	D-Link相关设备	CWE-284：访问控制不当	攻击者可以访问用户的私人信息，如照片等。
	婴儿监视器Mi-Cam	CWE-284：访问控制不当	攻击者可以监视用户。
	TOTOLINK路由器	CWE-20：输入验证不当	攻击者可以在设备中植入后门。
	路由器TP-Link	CWE-284：访问控制不当	攻击者可以获得root权限并将设备变为僵尸网络的节点。



## 小结

随着物联网设备种类日益繁多，攻击者的目标也会越来越丰富。如果读者对其他设备的漏洞感兴趣的话，请访问我们的最新[文章](#)。此外，您也可以阅读[Safegadget](#)、[Exploit IoT Hacks](#)方面的文章。

如您所见，这些类型的漏洞都很常见，并且大多数漏洞都属于应用程序安全的范畴。其中，某些设备甚至因为这些漏洞而变成僵尸网络的一部分。

美国国家标准与技术研究院最近发布了一份关于国际物联网国际网络安全标准化（IoT）状态的[白皮书](#)，其中列出了用以提高软件安全的软件保障标准以及相关指南。此外，

参考文章：

- [“How to Test the Security of IoT Smart Devices” by Infosec Institute](#)
- [OWASP IoT Top Ten Infographic](#)

点击收藏 | 1 关注 | 2

[上一篇：Z-Blog两处Getshell分...](#) [下一篇：对某cms过滤函数的突破及思考](#)

1. 2 条回复



[mss\\*\\*\\*\\*](#) 2018-04-15 17:25:47

原来建立表格也很简单，做个记号：

设备类型	设备名称	CWE	安全影响
-	::	::	-:
![图片.png](https://xzfile.aliyuncs.com/media/upload/picture/20180415172330-a95f4ddc-408e-1.png)	Heatmiser恒温器	CWE-598：通过GET请求中的查询字符串泄露信息	攻击者可以访问设备的所有设置，进而根据攻击者的意愿来随意更改各种设置，例如时间或温度。
![图片.png](https://xzfile.aliyuncs.com/media/upload/picture/20180415172330-a9675284-408e-1.png)	工业无线接入点Moxa AP	CWE-79：网页生成过程中没有对输入进行严格过滤（跨站脚本漏洞）	攻击者可以获得经过认证的会话，并且该会话永不过期。

0 回复Ta





[hi2994\\*\\*\\*\\*@aliyu](#) 2018-04-15 18:39:47

ssssssddddd

0 回复Ta

---

[登录](#) 后跟帖

[先知社区](#)

---

[现在登录](#)

[热门节点](#)

---

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)