OWASP
Open Web Application
Security Project

OWASP Iot Top 10 2018

- 祝书博

什么是IOT

物联网（IoT，Internet of things）
即“万物相连的互联网”，是互联网基础上的延伸和扩展的网络，将各种信息传感设备与互联网结合起来而形成的一个巨大网络，实现在任何时间、任何地点，人、机、物的互联互通。

物联网是新一代信息技术的重要组成部分，IT行业又叫：泛互联，意指物物相连，万物万联。由此，“物联网就是物物相连的互联网”。这有两层意思：第一，物联网的核心和基础仍然是互联网，是在互联网基础上的延伸和扩展的网络；第二，其用户端延伸和扩展到了任何物品与物品之间，进行信息交换和通信。因此，物联网的定义是通过射频识别、红外感应器、全球定位系统、激光扫描器等信息传感设备，按约定的协议，把任何物品与互联网相连接，进行信息交换和通信，以实现对物品的智能化识别、定位、跟踪、监控和管理的一种网络。

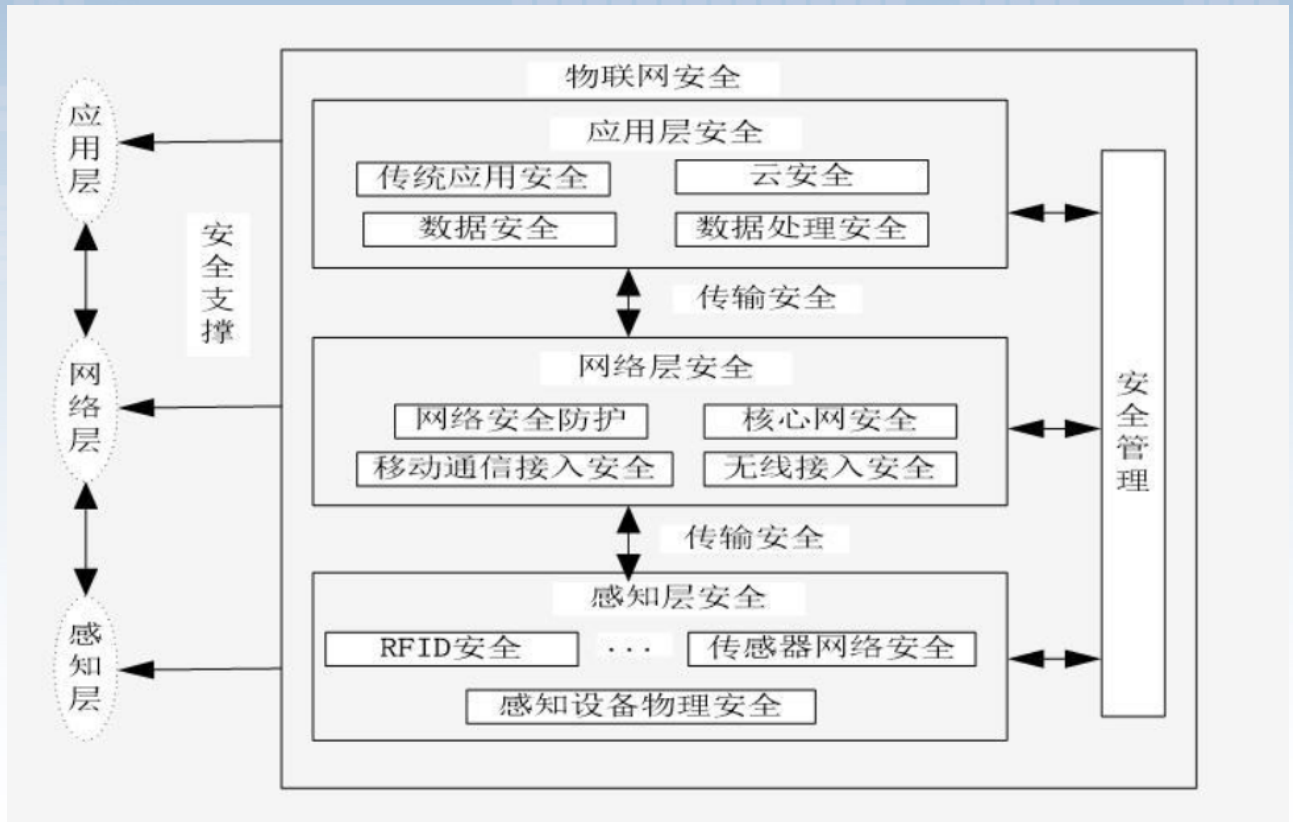
物联网三层架构

是物联网和用户（包括人、组织和其他系统）的接口。

由各种私有网络、互联网、有线和无线通信网、网络管理系统和云计算平台等组成。

由各种传感器以及传感器网关构成。

物联网安全



OWASP iot top 10

附录三：OWASP IoT TOP 10 2014

- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

截止时间：2019年6月4日

OWASP
Open Web Application Security Project

OWASP iot top 10 2018

OWASP IoT 项目作者

项目负责人

- Daniel Miessler
- Craig Smith
- Vishruta Rudresh
- Aaron Guzman

贡献者

- Justin Klein Keane
- Saša Zdjelar

IoT Top 2018贡献者

- Vijayamurugan Pushpanathan
- Alexander Lafrenz
- Masahiro Murashima
- Charlie Worrell
- José A. Rivas (jaxy)
- Pablo Endres
- Ade Yoseman
- Cédric Levy-
- Jason Andres
- Amélie Didio

原文文档

https://www.owasp.org/index.php/OWASP_Internet_of

OWASP IoT 项目中文版介绍

本文档为《OWASP Internet of Things (IoT) Top 10 2018》的中文版。本文档尽量保留原版本的格式和风格，但部分语言调整为中文习惯，其中存在的差异，尽请谅解。

为了方便阅读和理解本文档的内容，本手册对原英文版本的章节进行了调整，致使本手册的章节编号、页码与原英文版本的章节编号和页码不同。

特此感谢参与本文档工作的贡献团队与个人，以及其他关注和支持本项目的OWASP中国企业会员以及个人会员。

翻译：360代码卫士团队：申少华、韩建、章磊

开源网安团队：曹传勇、张海春

校验：王颉、Rip

编排：许飞

OWASP
Open Web Application Security Project

Top 1

弱密码、可猜测密码或硬编码密码

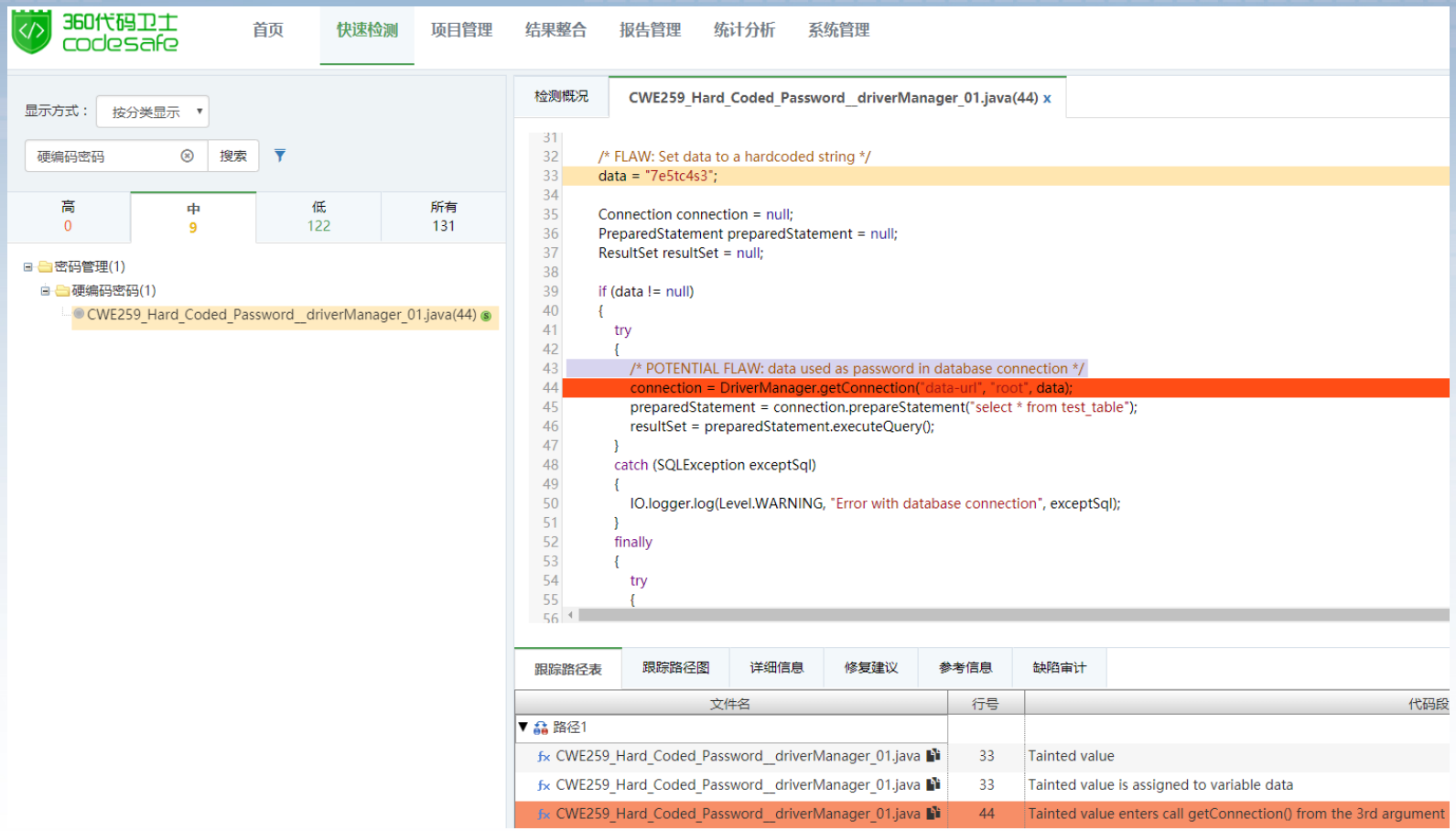
使用轻易可遭暴力破解的、可公开获取的或无法更改的凭证，包括固件或客户端软件中允许对已部署系统进行未经授权访问的后门。

A.摄像头弱口令

密码破解是摄像头最常用的攻击方式，一般利用厂家的默认密码。

以下为部分厂家摄像头的最常使用的十大默认用户名/密码：

十大默认用户名/密码	
admin/admin	Admin/1234
admin/1234	admin/123456
admin/<无密码>	admin/password
admin/12345	root/pass
root/<无密码>	root/camera



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	几乎任何人都可以访问DVR的设置，因为登录名和密码都是空的。
	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，控制报警装置的开/关状态，并激活报警装置的报警功能。
	DblTek 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，比如关闭GoIP。
	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摄像机的相关设置来监视用户。
	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，让摄像头加入Mirai之类的僵尸网络或仅用于监视用户。
	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信息。
	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，激活坐浴盆或风干功能，引起用户不适或危及人身安全。
	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，如发送虚假的高度或速度之类的飞行数据。
	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。

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。

Top 2

不安全的网络服务

设备运行了一些不需要或不安全的网络服务，尤其是那些暴露在互联网上的服务。它们会损害信息的保密性、完整性、真实性、可用性，或允许未经授权的远程控制。

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
	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，这会导致相当痛苦的体验甚至引起身体伤害，如引发突然的肌肉条件反射、皮肤烧伤，甚至神经损或导致死亡。
	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，从而导致电池耗尽和/或不适当的起搏或电击。
	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。
	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的大小（经典的缓冲区溢出漏洞）	在摄像机上执行远程代码。该漏洞可能导致用户个人数据泄露。
	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。
	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。
	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，并可以访问整个文件系统。

Top 3

不安全的生态接口

设备外生态系统中不安全的web、后端API、云或移动接口，导致设备或相关组件遭攻陷。常见的问题包括缺乏认证/授权、缺乏加密或弱加密以及缺乏输入和输出过滤。

Web接口，云接口，移动设备接口

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，进而根据攻击者的意愿来随意更改各种设置，例如时间或温度。
	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。
	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（跨站脚本漏洞）&CWE-89：没有对SQL命令中的特殊元素进行严格过滤（SQL注入漏洞）	攻击者可以劫持手机，并窃取敏感的个人数据。
	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，如用户密码。
	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（跨站脚本漏洞）	攻击者可以读取存储在操作系统中的所有文件。此外，攻击者还可以修改设备的配置，上传任意更新。
	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（跨站脚本漏洞）	攻击者可以通过基于Web的命令来控制设备的所有功能。
	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（跨站脚本漏洞）	攻击者可以在设备上植入存储型XSS代码，进而使管理员在浏览器中执行任意JavaScript代码。
	Hanbanggaoke网络摄像头	CWE-650：信任服务器端的HTTP权限方法	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来控制该路由器，修改其DNS设置，并将浏览器重定向到恶意站点。

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
	Seagate Personal Cloud Home Media Storage	CWE-598：通过GET请求中的查询字符串泄露信息	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。

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，即使加密算法具有足够的加密强度，仍然可能存在缺乏双因子身份验证，或者允许用户使用弱密码等安全漏洞。

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-287：不恰当的身份验证	攻击者可以访问用户的个人数据，包括清晰的图像、聊天记录、性取向、电子邮件地址和明文密码
	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，打开音频、麦克风和扬声器与儿童进行交流，或者肆意地访问儿童卧室的实时录像。
	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，并于原软件所在位置安装恶意软件。
	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进行操作。
	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。

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。

Top 4

缺乏安全的更新机制

缺乏安全更新设备的能力，包括缺乏对设备固件的验证、缺乏不安全的交付（未加密的传输）、缺乏防回滚机制以及缺乏对更新的安全变更的通知。

Top 5

使用不安全或已遭弃用的组件

使用已遭弃用的或不安全的软件组件/库，将导致设备遭攻陷。组件包括操作系统平台的不安全定制以及使用来自受损供应链的第三方软件或硬件组件。

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的一部分。
	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相关配置	攻击者可以完全控制设备，例如，打开设备并使其长期工作，这可能会引发火灾。
	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。

Top 6

隐私保护不充分

存储在设备或生态系统中的用户个人信息被不安全的、不当的、或未经授权的使用。

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、定位方法（GPS与Wi-Fi）、位置坐标、电池电量等信息。
	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，或使其成为僵尸网络的一部分。
	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上。
	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。

Top 7

不安全的数据传输和存储

缺乏对生态系统中任何位置的敏感数据进行加密或访问控制，包括：未使用时、传输过程中或处理过程中的敏感数据。

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-F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权限。
	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用户的凭证。
	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，以恢复密钥并解密通信流量。
	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）	攻击者可以向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。

Top 8

缺乏设备管理

对已部署在生产过程中的设备，缺乏安全支持，包括：资产管理、更新管理、安全接触、系统监控和响应能力。

Top 9

不安全的默认设置

设备或系统的默认设置不安全，或缺乏限制操作者修改配置的方式让系统更加安全的能力。

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相关配置	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，这使得它们可以在互联网上轻松搜索到。
	Canon打印机	CWE-269：权限管理不当 & CWE-295：证书验证不当	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。

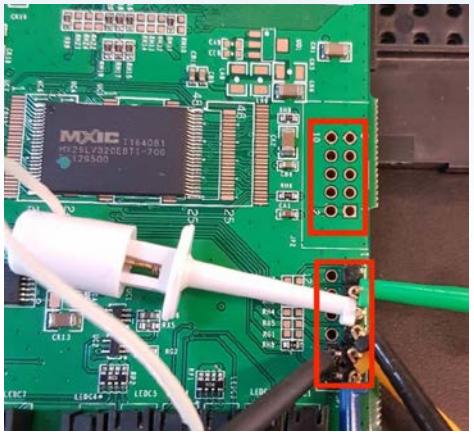
Top 10

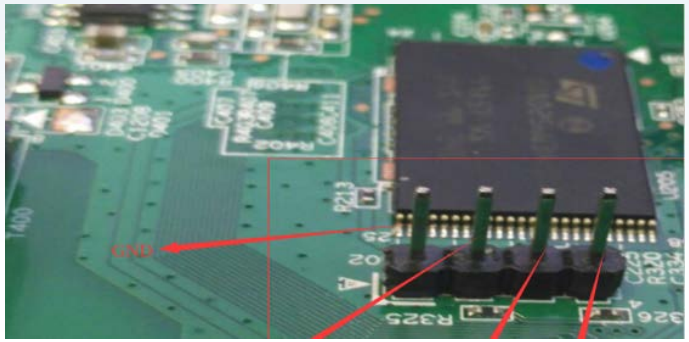
缺乏物理加固措施

缺乏物理加固措施，导致潜在攻击者能够获取敏感信息以便后续进行远程攻击或对设备进行本地控制。

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一部分。
	Smart Nest恒温器	CWE-284：访问控制不当	攻击者可以从外设（例如USB或UART）启动处理器。





OWASP中国区部分项目

- OWASP项目
  - OWASP Mobile Security
  - 招聘专区
  - 2017 OWASP TOP 10
  - OWASP Internet of Things项目
  - 安全基线项目
  - OWASP ZAP项目
  - OWASP中国资源池
  - OWASP Newsletter翻译
  - OWASP ESAPI项目
  - OWASP Live CD
  - WebGoat
  - OWASP风险评级方法
  - OWASP SAMM
  - OWASP Cloud-10 Project
- OWASP AntiSamy. Java
- OWASP AntiSamy.Net
- WAF测试基准项目
- 在线网络安全攻防实验室
- OWASP安全编码指南
- 代码安全项目
- OWASP中国会员积分制（试行）
- OWASP中国WAF调查问卷
- 2013 OWASP Top 10
- OWASP应用程序安全设计项目
- 首席安全官（CISO）应用安全指南
- OWASP CISO Survey 2014 项目
- 众测行业规范
- OWASP 测试指南
- OWASP蛇梯棋项目
- 十大移动应用恶意行为
- BSIMM6 文档翻译 项目团队召集书
- ModSecurity项目
- 轻量级应用安全开发生命周期项目（S-SDLC）
- 数据库审计系统测评基准
- 静态源代码安全分析工具测评基准
- <OWASP TOP 10 深度解析>项目
- OWASP ProActive Controls中文项目
- OWASP无服务器应用安全风险TOP 10
- 区块链安全TOP10

OWASP
Open Web Application
Security Project