OWASP TOP 10
INTERNET OF THINGS 2018

OWASP IoT 项目 2018

OWASP中国
2019年1月

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 (jarv)
- Pablo Endres
- Ade Yoseman
- Cédric Levy-Bencheotn
- Jason Andress
- Amélie Didion - Designer

原文文档

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

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

本文档主要分成以下三部分

OWASP IoT TOP 10 2018

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带有允许对已部署系统进行未经授权访问的后门。

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。

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或授权、缺乏加密或弱加密以及缺乏输入和输出过滤。

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、缺乏安全交付（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。

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。

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。

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。

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、安全解除、系统监控和响应能力。

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。

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。

OWASP IoT TOP 10项目-理念

OWASP IoT项目始于2014年，旨在帮助开发人员、制造商、企业和消费者在创建和使用IoT系统时做出更好的决策。

2018年发布的OWASP IoT Top 10的也延续了这一理念。OWASP IoT TOP 10代表了构建、部署或管理IoT系统时需要避免的十大事项。《OWASP IoT TOP 10 2018》的主旋律是简洁。本OWASP项目团队为开发人员、企业和消费者筛选形成了一个单一的、统一的列表来展现在处理物联网安全时需要避免的最重要事项，而不是针对风险、威胁和漏洞创建的单独列表。

本OWASP项目团队认识到：现在有几十个组织发布了关于物联网安全的详细指南，所有这些指南都是为有不同的受众和行业垂直领域设计的。本OWASP项目团队认为可以创建的最有用的资源，是一个能同时解决制造商、企业和消费者最高优先级问题的单一列表。

因此，输出了《OWASP IoT TOP 10 2018》文档。

OWASP IoT TOP 10项目-方法

本OWASP项目团队由来自于安全行业的专业志愿者组成，他们的经验跨越多个专业领域，包括：制造商、咨询、安全测试人员、开发人员等。

本项目分以下几个阶段进行：

团队组建

- 寻找愿意为OWASP IOT TOP 10 2018更新做出贡献的人员，包括中小企业和项目负责人，他们将在项目期间执行各种任务。

项目回顾

- 对“OWASP IoT TOP 10 2014”项目进行分析，以确定自该版本发布以来，行业中发生了哪些变化，以及如何根据这些变化更新列表。

数据收集

- 收集和审查多个漏洞来源(公共和私人)，特别着重于哪些问题造成了最严重的实际影响和损害。

同类型项目评审

- 对数十个其他物联网安全项目进行评审，以确保没有遗漏重要内容，并对发布的内容和优先级感到满意。其他物联网安全项目包括：CSA物联网控制矩阵、CTIA、斯坦福物联网安全项目、NISTIR 8200、ENISA物联网基线报告、消费者物联网安全时间准则等。

社区草案反馈

- 将草案发布给社区进行审查，包括多次在Twitter上征求意见、使用公共反馈表以及收集反馈意见的一些公开访谈。然后，团队在最初的数据收集以及同类型项目评审的同时，对反馈进行评审，以创建列表内容和优先级。

发布

- 项目于2018年12月向公众发布。

本OWASP项目团队已经计划了一些活动来持续改进项目。

讨论的一些项目包括:

✓ 以两年为周期，持续优化本Top 10列表，收集社区和其他项目贡献者的反馈，以确保我们能及时了解行业面临的问题;

✓ 将列表项映射到其他OWASP项目，如：OWASP ASVS，也可能映射到OWASP之外的其他项目;

✓ 将项目扩展到其他方面，包括：嵌入式安全、ICS/SCADA等;

✓ 添加使用和滥用案例，并提供多个示例，以巩固所讨论的每个概念;

✓ 考虑到参考体系结构的增加，我们不仅可以告诉人们应该避免什么，而且还可以告诉人们如何安全地做他们需要做的事情。

对OWASP全球社区开放参与OWASP IoT 项目。我们从所有参与者那里获取建议——无论您是开发人员、制造商、渗透测试人员，还是只是想安全地实施物联网的人。您可以每隔一个周五在OWASP Slack Channel的#iot-security会议室参与团队会议。

OWASP IoT 安全团队，2018

OWASP Internet of Things (IoT) Project

牛津字典将物联网“Internet of Things”定义为：“一种拟议中的互联网发展，在这种发展中，日常物品具有网络连接，从而发送和接收数据。”

OWASP IOT项目旨在帮助制造商、开发人员和消费者更好地理解与物联网相关的安全问题，并确保无论在任何环境中，用户都能够在构建、部署或评估物联网技术时，做出更好的安全决策。

该项目旨在为各种物联网子项目定义一个架构，例如攻击面区域，测试指南和高危漏洞。

附录一：IoT攻击面项目-2014

IoT攻击面项目提供了制造商、开发人员、安全研究人员以及希望在其组织内部署或实现IoT技术的人员应该了解的攻击面列表。

攻击面	漏洞
生态系统	• 互操作性标准 • 数据治理 • 系统故障 • 个人利益相关者风险 • 组件之间的隐式信任 • 注册安全 • 退役系统 • 丢失的访问过程
设备内存	• 敏感数据 ◦ 明文用户名 ◦ 明文密码 ◦ 第三方凭证 ◦ 加密密钥
设备物理接口	• 固件提取 • 用户CLI • 管理员CLI • 特权升级 • 重置为不安全状态 • 防篡改 • 设备ID、序列号曝光 • 删除存储介质 ◦ 调试端口 ◦ UART(串口) ◦ JTAG/SWD
设备Web界面	• 标准的 Web 应用程序漏洞集, 请参见： ◦《OWASP Top 10》 ◦《OWASP ASVS》 ◦《OWASP测试指南》 • 凭证管理漏洞： ◦ 用户名枚举 ◦ 弱密码 ◦ 账户锁定 ◦ 已知的默认凭证 • 不安全的密码恢复机制
设备固件	• 敏感数据泄漏 (见 2013年版或2017年版《OWASP Top 10》中 “A6 敏感数据泄漏” 部分内容)： ◦ 后门账户 ◦ 硬编码凭据 ◦ 加密密钥 ◦ 加密 (对称、不对称) ◦ 敏感信息 ◦ 敏感的 URL泄漏 • 易受攻击的服务 (如：Web、SSH、TFTP等) ◦ 验证旧的 SW版本和可能受到的攻击 (Heartbleed、Shellshock、旧的 PHP版本等) • 固件版本和最近更新日期显示 • 与安全相关功能的API 泄漏 • 固件降级

攻击面	漏洞
设备网络服务	• 信息泄露 • 用户CLI • 管理CLI • 注入 • 拒绝服务 • 非加密服务 • 弱加密 • 测试、开发服务 • 缓冲区溢出 • UPnP • 易受攻击的UDP服务 • DoS攻击 • 设备固件OTA更新阻止 • 通过不安全通道加载的固件（无TLS） • 攻击重演 • 缺乏有效载荷验证 • 缺乏信息完整性检查 • 证书管理漏洞 • 不安全的密码恢复机制 ◦ 用户名枚举 ◦ 弱密码 ◦ 账户锁定 ◦ 已知的默认凭证
管理界面	• 安全/加密选项 • 记录选项 • 双因素身份验证 • 检查不安全的直接对象引用 • 无法擦拭设备 • 标准的Web应用程序漏洞，请参阅： ◦《OWASP Top 10》 ◦《OWASP ASVS》 ◦《OWASP测试指南》 • 证书管理漏洞： ◦ 用户名枚举 ◦ 弱密码 ◦ 账户锁定 ◦ 已知的默认凭证 ◦ 不安全的密码恢复机制
本地数据存储	• 未加密数据 • 使用发现的密钥来加密数据 • 缺少数据完整性检查 • 使用静态相同的enc / dec键
云Web界面	• 标准的Web应用程序漏洞，请参阅： ◦《OWASP Top 10》 ◦《OWASP ASVS》 ◦《OWASP测试指南》 • 证书管理漏洞： ◦ 用户名枚举 ◦ 弱密码 ◦ 账户锁定 ◦ 已知的默认凭证 ◦ 不安全的密码恢复机制 • 传输加密 • 双因素身份验证
第三方后端APIs	• 未加密PII发送 • 加密PII发送 • 设备信息泄露 • 位置泄漏
更新机制	• 未加密更新发送 • 未签名更新 • 更新位置为可写 • 更新验证 • 更新认证 • 恶意更新 • 缺乏更新机制 • 不支持手动更新机制
移动应用程序	• 设备或云端的隐性信任 • 用户名枚举 • 账号锁定 • 已知默认凭证 • 弱密码 • 不安全的数据存储 • 传输加密 • 不安全的密码恢复机制 • 双因素认证
供应商后端API	• 云或移动应用的内置信任 • 弱认证 • 弱访问控制 • 注入攻击 • 隐藏服务
生态系统通信	• 健康检查 • 心跳 • 生态系统命令 • 取消配置 • 推送更新
网络流量	• LAN • 局域网到互联网 • 短范围 • 非标准 • Fuzzing协议 • 无线（WiFi、Z波、XBee、Zigbee、蓝牙、LoRA）
认证与授权	• 认证、授权相关值（如：会话密钥、令牌、cookie等）泄露 • 重新使用会话密钥、令牌等 • 设备到设备的认证 • 设备到移动应用程序的认证 • 设备到云系统的认证 • 移动应用程序到云系统的认证 • Web应用程序到云系统的认证 • 缺乏动态认证
隐私	• 用户数据泄露 • 用户/设备位置暴露 • 差异化隐私
硬件（传感器）	• 感知环境操作 • 篡改（物理上） • 损害（物理上）

附录二：IoT漏洞项目-2014

“IoT漏洞项目”，内容包括最严重的物联网漏洞信息、和漏洞相关联的攻击面以及对漏洞的概述。

具体如下：

漏洞	攻击面	概要
用户名枚举	• 管理界面 • 设备Web界面 • 云界面 • 移动应用程序	• 能够通过认证交互收集一组有效的用户名。
弱密码	• 管理界面 • 设备Web界面 • 云界面 • 移动应用程序	• 例如，允许将账户密码设置为“1234”或“123456”。 • 使用预先编程的默认密码。
账号锁定	• 管理界面 • 设备Web界面 • 云界面 • 移动应用程序	• 能够在3至5次登录尝试失败后，继续发送身份验证尝试。
非加密服务	• 设备网络服务	• 网络服务未作适当加密来防止攻击者窃听或篡改。
双因素认证	• 管理界面 • 云Web界面 • 移动应用程序	• 缺少双因素认证机制，例如安全令牌或指纹扫描器。
轻度加密	• 设备网络服务	• 虽然已执行加密，但是该配置不正确或未被能准确更新。例如使用SSL v2。
非加密更新	• 更新机制	• 更新是在没有使用TLS或加密情况下通过网络传输更新文件的。
更新位置为可写	• 更新机制	• 更新文件的存储位置为可写，并允许修改固件并分发给所有用户。
拒绝服务	• 设备网络服务	• 服务能够以拒绝该服务或整个设备的服务方式进行攻击。
删除存储介质	• 设备物理接口	• 能够从设备中删除物理存储介质。
无手动更新机制	• 更新机制	• 无法手动强制更新检查设备。
缺乏更新机制	• 更新机制	• 无法更新设备。
固件版本显示及最后更新日期	• 设备固件	• 当前固件版本不显示，或者最后更新日期不显示，也有可能两者都不显示。
固件和存储提取	• JTAG / SWD接口 • In-Situ dumping • 拦截OTA更新 • eMMC敲击 • 从制造商网页进行下载 • 取消链接SPI Flash / eMMC芯片并在适配器中进行读取	• 固件包含许多有用的信息，例如，运行服务的源代码和二进制文件、预设密码、ssh密钥等。
操纵设备的代码执行流程	• JTAG / SWD接口 • 侧面渠道攻击，如：Glitching攻击。	• 借助于JTAG适配器和gdb，我们可以修改设备中固件的执行程序，并绕过几乎所有基于软件的安全控制。 • 侧面通道攻击还可以修改执行流程，或者可以用来获取设备泄漏的有趣信息。
获取控制台访问	• 串行接口（SPI / UART）	• 通过连接到串行接口，我们将获得对设备的完全控制台访问。 • 通常来说，安全措施包括防止攻击者进入单独用户模式的自定义启动程序，但它也可以绕过攻击者。
不安全的第三方组件	• 软件	• 使用过期版本的busybox、openssl、ssh、web服务器等。

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

附录四：OWASP 中国

联系我们

会员：member@owasp.org.cn

项目：project@owasp.org.cn

微信：OWASP_China

官网：www.owasp.org.cn