

双管齐下堵住智能音箱安全漏洞

中国软件评测中心 左冉 王琦 曹顺超

近年来,智能音箱等智能家居产品逐渐走入千家万户,为人们的居家生活增添了便利和乐趣。IDC发布的《中国智能音箱零售市场月度追踪》报告显示,2021年中国智能音箱市场销量为3654万台,同比增长20.1%,预计2022年市场销量将达到3725万台。

智能音箱正在向有屏、无屏音箱持续分化:一种是在传统智能音箱上进一步升级,通过增加屏幕、摄像头,逐渐向家用平板、智慧屏靠近。另一种则是进一步轻量化、无线化和模块化,主要定位智能家居的智能音频控制、交互入口,未来智能音箱将继续渗透,嵌入更多家居产品、家电内。随着智能音箱功能逐渐多元化,信息技术手段愈发复杂,其安全风险也渐渐浮出水面。

智能音箱安全风险不容小觑

智能音箱安全风险主要分为两个方面。一是随着智能音箱所集成的功能多样化、交互接口数量增长,可能被攻击的入口逐渐增多,安全风险不断扩大。2019年,Google Home被攻破,攻击者可以通过远程指令操控目标设备。如果事件一旦升级,可能导致数百万用户个人信息泄露,轻则导致用户遭受诈骗、资金被盗用,重则导致用户的人身安全受到威胁,影响社会稳定。

二是智能音箱产品定位及个性化功能产生的需求,导致其收集了大量用户隐私信息及交互数据,由此可能产生违规收集用户个人数据的安全隐患。2019年,有媒体披露亚马逊雇佣数千员工监听旗下智能音箱Amazon Echo用户的日常录音,甚至违规泄露1700多个用户的语音数据,导致用户不知不觉间受到电商骚扰、电信诈骗等一系列影响。

中国软件评测中心选取了市面畅销的多台有屏智能音箱和无屏智能音箱,从网络安全、数据安全和个人信息安全等多个角度进行测评。

智能音箱网络安全与数据安全。智能音箱APP安全。测评专家对智能音箱APP的安全性进行了测试,包括组件安全检测、Manifest文件检测、Webview安全检测、网络通信安全检测、弱加密风险检测、数据安全检测、系统漏洞检测、so文件风险检测、隐私权限检测、隐私行为检测等测试项。在测试过

程中,专家通过对apk文件进行反编译,采用自动化扫描与人工渗透相结合的技术手段以发现其存在的安全问题。

经测评,测评范围内的智能音箱APP均未检测出严重漏洞,能够有效避免用户信息泄露。

智能音箱通信数据传输安全。测评专家在智能音箱系统与服务器端的通信过程中,动态采集传输的网络数据。在针对智能音箱联网通信和连接维护全过程的加密算法方面,使用Wireshark工具和人工审计的方式,进行了安全分析和评估。

经测评,某智能音箱设备在与服务器端进行通信过程中,存在日志文件明文传输,导致用户敏感信息泄露等问题。传输的日志中包含设备信息、日志信息和语音转换出的文本信息,造成信息泄露。

智能音箱系统与固件升级安全。测评专家首先对智能音箱系统与固件做了降级风险测试,发现大部分设备采取了“升级检测”和“固件签名”的措施,锁定了串口和USB接口,用户无法自行降级,保护了智能音箱的安全。其次,专家对智能音箱固件更新请求通信过程进行了分析,通过分析更新请求数据包,发现部分设备通过HTTP协议明文传输固件升级请求。从数据包中可以获取固件下载地址,引发固件泄露风险。同时,使用不安全的通信协议可能面临中间人攻击的风险。

经测评,部分智能音箱固件升级通信过程存在URL暴露风险,可能发生固件泄露事件。

智能音箱用户个人信息安全。个人信

息收集使用规则。为了给用户提供更加精准的定制化服务,智能音箱会收集用户的个人信息,包括位置信息、通信录信息、音视频信息等敏感数据。中国软件评测中心对多款音箱的个人信息收集使用规则进行了合规性检测。

在对个人信息收集使用规则进行检测的过程中,测评专家主要对各智能音箱产品的隐私政策进行了详细解读,并对其中存在的一些疑问与企业进行了访谈。参与测评的智能音响产品都拥有完整的个人信息保护政策,并且能够在实际应用中付诸实践。

但智能音箱在收集使用个人信息的过程中,仍存在过度收集用户个人信息的情况。例如,在进入智能音箱APP之后,会自动收集用户语音数据用于模型训练,但未对用户进行明显提示。部分产品的隐私声明未对个人信息的采集频率以及存储时间进行明确说明。

个人信息主体注销账户。用户对智能音箱存储的个人用户信息应该完全可控,在用户要求进行账户注销或用户数据销毁时,智能音箱、控制端APP或云端服务应向用户提供简单便捷的操作方式,并且在注销过程中不应设置不合理的条件或提出额外要求增加个人信息主体义务,如注销单个功能视同注销主体账号,要求个人信息主体填写精确的历史操作记录作为注销的必要条件等。

经过对参与测评的智能音箱产品进行检测,部分智能音箱账户注销及用户数据销毁仍存在难题。当用户注销智能音箱账户时,会将此账户下所有产品及服务注销,使



对智能音箱生产企业和使用者的建议

中国软件评测中心针对以上测评内容,从企业和用户的角度出发为智能音箱安全建设提出建议。

对智能音箱生产企业的建议。首先,加强产品网络和数据安全合规建设。在网络安全层面,可以从以下三个方面加强产品的安全保障,一是对于智能音箱操作系统的漏洞及时进行修复,加强系统配置安全和端口安全管理;二是对系统固件和移动应用进行安全加固,包括但不限于签名校验、加壳、防内存修改等手段;三是在服务器端和智能音箱APP引入并重视安全测试,定期开展渗透测试和风险评估。

在数据安全层面,应落实数据安全法、个人信息保护法的相关规定,进行数据全生命周期安全防护,做到收集信息应授权、传输存储应加密、加工使用应脱敏、删除数据应彻底、提供公开应合法。

其次,规范对用户个人信息的收集使用规则。产品在收集用户个人信息等方面应不具备强制性,根据功能将用户信息收集模块化,不因某信息用户未授权而拒绝提供服务。

在收集、使用用户个人信息过程中,应对收集信息的内容、方式、范围、目的、频次、精准度等进行详细说明,其中,对于用户敏感信息的收集,应有明显提示;对于个人信

息的使用,如是否会向第三方、境外提供数据应进行详细说明;对于个人信息的撤销授权、申请删除、投诉举报的渠道和方法,应提供全面且便于理解的操作说明。

对智能音箱用户的建议。首先,关注产品收集使用个人信息规则。可以从以下两个方面进行:一是关注注册信息,在隐私协议中详细查阅产品收集的内容、目的、频次、精确度等,并明确其加工、使用、第三方共享的条款内容,保障自身利益;二是注册并登录后,进入设置或用户授权管理等页面,查看产品授权信息,并依据需求关闭敏感信息的授权。如遇强制收集或违法使用个人信息的情况,应及时向监管部门进行举报。

其次,关注账号信息安全。智能音箱控制端账号通常为多APP、多产品共用。智能音箱作为智能家居的控制入口之一,具备控制其他设备的功能,其账号一旦泄露或被窃取,登录了其他智能音箱设备,安全风险会通过智能音箱放大,造成更大威胁。账号密码应具备一定复杂度并定期更换,避免与其他账户共用密码,不要点击他人发送的可疑链接。

最后,关注废旧设备个人信息处理。智能音箱设备即便已经丢弃,但存在里面的数据仍有泄露的风险。经测评发现,多个品牌智能音箱在离开主人并接入新的网络环境后,未经验证即可正常控制原账号下绑定的设备,甚至部分有屏音箱,可以直接查看其绑定的摄像头。建议用户在丢弃产品前退出个人账户、删除设备信息或重置设备,同时选取较为安全的丢弃方式,如选择可靠的废旧电子设备回收机构。

中国电子报

一报在手 行业在握

融媒体服务

- 报纸出版
- 官方网站（电子信息产业网www.cena.com.cn）
- 官方微信（公众号cena1984）
- 官方微博(http://weibo.com/cena1984)
- 视频平台（抖音、快手、央视网、人民视频等）

- 视频服务（视频制作、在线直播、在线会议等）
- 平台推广(学习强国、今日头条、百度百家等)
- 内参专报
- 行业报告
- 图书出版

会赛展服务

- 会议活动
- 专业大赛
- 展览展示
- 专业培训
- 政府服务

- 企业定制
- 产品评测
- 舆情监测
- 数据营销
- 招商引资

官方微信

官方网站

在这里

让我们一起把握行业脉动

www.cena.com.cn

地址：北京市海淀区紫竹院路66号赛迪大厦18层

电话：010-88558808/8838/9779/8853

传真：010-88558805

广告