智能摄像头
安全能力白皮书
(2020.V2.1)

目录

前言

近年来随着物联网、智能家居等业态的快速发展，智能看家(网络摄像头及门铃猫眼)设备也增长迅速。随着智能看家设备产业规模的逐渐扩大，这些设备带来的安全问题也逐渐凸显。越来越多的实际案例在提醒大众，智能看家设备若自身出现安全问题将会造成很多风险，如远程控制，隐私监视等，智能看家设备的安全加固也是迫在眉睫。

文中提出的基于摄像头及门铃/猫眼产品在硬件、设备软件、产品功能等方面的安全技术能力适用于我司目前产品，包括但不限于：

1.室内安防摄像机：ZNIPC-418DJ-IR、ZNIPC-317DJ-IR、ZNIPC-206DJ-IR、ZNIPC-306DJ-IR、ZNIPC-207EC-IR、HDC-50、HDC-52、HDC-56、HDC-57、IPC-Y31-WU-IR、HM-IPC-Y31-WU-IR。

2.室外安防摄像机：ZNIPC-418W-IR、ZNIPC-419W-IR、ZNIPC-317W-IR、ZNIPC-207W-IR、ZNIPC-405DJ-IR、IPC-PT31-EP-W、HM-IPC-PT31-EP-W、ZN-YLB100-IR.

3.门铃以及猫眼产品：ZNVD-295C-IR、ZNVD-296C-IR、ZNPH-202C-IR。

第一章 范围

本文档规定了安防摄像头及门铃/猫眼设备的安全能力技术要求，包括物理硬件层、固件系统层、网络通信层、应用数据层安全能力。文中提到的技术能力适用于我司目前所有的安防摄像头及门铃猫眼设备。

第二章 规范性引用文件

2.1 引用文件

下列标准所包含的条文，通过本规范的引用而构成本规范的条文。在规范出版时，所示版本均为有效，所有标准都可能推出更新版本。使用本规范的各方应探讨使用下列标准最新版本的可能性：

a) GB/T 35273 《个人信息安全规范》；

b) GB 35114-2017 《公共安全视频监控联网信息安全技术要求》;

c) GB 4943.1-2011 或 GB 8898-2011《信息技术设备安全》检测标准规范要求。

2.2 缩略语

下列缩略语适用于本文件

CTEI 中国电信设备标识(China Telecom Equipment Identity)

IMSI 国际移动用户识别码(International Mobile Subscriber Identification Number)

IMEI 国际移动设备识别码(International Mobile Equipment Identity)

TEE 可信执行环境(Trusted Execution Environment)

CNVD 国家信息安全漏洞共享平台(China National Vulnerability Database)

CNNVD 国家信息安全漏洞库(China National Vulnerability Database of Information Security)

TLS 传输层安全协议(Transport Layer Security)

DTLS 数据包传输层安全性协议(Datagram Transport Layer Security)

RTSP 实时流传输协议(Real Time Streaming Protocol)

第三章 设备安全能力框架

图 1 为智能网络摄像头类设备安全能力框架，主要包含 4 个部分：物理与硬件安全、固件与操作系统安全、网络与通讯安全、应用与数据安全。

图 1. 智能摄像头类设备安全能力框架

其中：

a) 物理与硬件安全能力：在物理硬件层面保障智能摄像头安全，具备相应的安全要求，从硬件接口、安全启动、抗攻击等层面保护智能摄像头；

b) 固件与系统安全能力：在固件与系统层面保障智能摄像头安全，具备相应的安全要求，从固件升级、密钥安全等层面保护智能摄像头；

c) 网络与通信安全：在网络与通信层面保障智能摄像头安全，保障智能摄像头采用有线、无线通信协议安全能力满足相应的国家标准或标准组织规定；

d) 应用与数据安全能力：在应用数据层面保障智能摄像头安全，保证数据的完整性、可用性、机密性。

第四章 安全能力规范

4.1 物理与硬件安全能力

4.1.1 可调式接口安全

a) 终端设备具有本地硬件调试接口或通信接口情况下，支持接口访问控制或关闭的能力；

b) 终端设备具有本地硬件调试接口或通信接口情况下，接口登录认证为强口令；

c) 禁用闲置的外部设备接口；

d) 禁用外接存储设备引导启动系统自启动功能。

4.1.2 启动安全

a) 支持设备安全启动的能力，默认安全启动。

4.1.3 存储芯片安全

a) 支持设备核心代码，核心报警模型的安全存储。

4.1.4 身份标识

a) 有明确的标识，如 CTEI、终端编号、接入用户号（如 IMSI）、接入模块号（如 IMEI 号）等；

b) 终端设备身份支持防篡改的唯一识别码的能力。

4.1.5 硬件实现密码算法

a) 终端设备支持使用 TEE 执行环境或独立的安全芯片进行密码运算。

4.2 固件与系统安全能力

4.2.1 固件保护

a) 设备启动时具备固件签名验证的能力；

b) 具备固件加固保护的能力。

4.2.2 系统防护

a) 支持终端设备操作系统最小化安装，仅安装必要的组件和应用程序的能力。

4.2.3 固件和系统升级安全

a) 设备支持固件和系统远程升级；

b) 设备升级时，支持对升级软件包进行数字签名验签；

c) 设备远程升级时，支持升级软件包安全传输到终端设备的能力；

d) 支持升级包更新之前进行完整性校验的能力，防止升级包传输过程被篡改；

e) 设备进行系统与固件更新，当发生因更新包缺陷而导致更新失败时，不会出现系统不可用的情况；

f) 设备支持防回滚，不会安装比当前版本更低的版本；

g) 设备支持存储芯片内固件签名校验。

4.2.4 漏洞修复

a) 系统不包含有 CNVD 与 CNNVD 6 个月前公布的高危漏洞；

b) 支持紧急系统缺陷及漏洞的两周内修复。

4.2.5 日志审计

c) 支持对设备主要操作进行审计；

d) 设备日志，针对用户关键信息脱敏，如 Token、云存空间号等信息。

4.2.6 密钥存储及证书安全

a) 本地密码加密存储，不以明文存储；

b) 摄像头与平台交互的业务数据的加解密密钥由安全的密钥生成算法生成；

c) 流媒体密钥由服务端分配，密钥与设备 ID 绑定，密钥和加密向量保存在设备端，设备用该密钥负责对实时码流、回放码流和上传云存的码流加密；

d) 摄像头证书加密保存在安全的存储区域。

4.3 网络与通信安全能力

4.3.1 网络接入认证

a) 在接入网络中具有唯一网络身份标识；

b) 能向接入网络证明其网络身份，支持基于对称或非对称密码机制的鉴别。

4.3.2 网络访问控制

a) 对远程登陆的用户具备身份认证能力；

b) 对远程用户的访问进行访问控制管理，管理不同用户所能访问的数据、访问权限和访问时效性；

c) 支持对应用层访问控制的能力；

d) 支持网络端口最小化暴露原则，并禁用闲置的通信端口；

e) 设置口令复杂度和禁止弱口令；

f) 支持终端设备与接入网络间双向认证的能力。

4.3.3 通信保护

a) 支持终端设备与接入网络间，以及对终端设备远程管理时采用通信机密性保护机制，实现鉴别数据、隐私数据和重要业务数据等数据的机密性保护，如使用 TLS，DTLS 等安全通信协议，加密算法应符合国家密码相关规定；

b) 支持终端设备与接入网络间，以及对终端设备远程管理时采用通信完整性保护机制，实现鉴别数据、隐私数据和重要业务数据等数据的完整性保护。

4.3.4 RTSP 服务安全

a) 网络摄像头及门铃猫眼 554 端口开放时会设置口令复杂度限制，禁止使用弱口令。

4.4 应用数据安全能力

4.4.1 Web 服务安全

a) 设备缺省关闭 web 服务功能，不允许用户通过 web 进行控制。

4.4.2 数据机密性

a) 支持对终端上的重要数据（如所有的密钥和私钥、身份验证和其他安全配置）和重要业务数据实施机密性保护，确保这些数据在存储和传输中的保密性；

b) 支持对采集的视频及音频进行加密操作并传输。

4.4.3 数据完整性

a) 支持对终端上的重要数据（如所有的密钥和私钥、身份验证和其他安全配置）和重要业务数据实施完整性保护，确保这些数据在存储和传输中的完整性。

4.4.4 数据可用性

a) 应提供摄像头类设备取证场景的的本地备份保存与重传功能。

兆能讯通
SuperElectron

深圳市兆能讯通科技有限公司成立于 2014 年，注册资金 2 亿元，是一家以智能视讯终端产品开发、设计、生产为核心，业务涵盖 IPTV/OTT 系统、智能机顶盒、智能网关、智能监控安防摄像头、语音蓝牙音箱、家庭媒体中心等网络智能终端设备及信息家电产品的国家高新技术企业。公司成立短短 5 年来，就已经在网络智能终端领域取得不凡业绩，2019 年销售额达 11.3 个亿，2020 年预计达 25 个亿。

公司研发实力丰富，各省分公司办事处 30 余省，在深圳、北京、上海、成都均设有研发基地，研发技术人员共计 200 多人，可以应对多种产品及不同客户的研发需求。

公司始终坚持走科技创新之路，累计获得多项国家专利授权，是行业内拥有知识产权技术较多的企业。公司获得国家高新技术企业认定，并通过 ISO9001 质量管理体系认证、 ISO14001 环境管理体系认证、中国职业健康安全管理体系认证、信息安全管理体系认证等各项管理体系认证。

http://superelectron.com.cn/

合作伙伴

中国电信 CHINA TELECOM　中国移动 China Mobile　China unicom 中国联通　中国银联 China UnionPay　CNR 中央人民广播电台　ziroom 自如 创 | 享 | 主 | 活