

DB32

江苏省地方标准

DB32/T 4432—2022

视频监控联网信息安全 自动化漏洞扫描技术规范

Information security of video monitoring network—
Technical specifications for automatic vulnerability scanning

2022-12-31 发布

2023-01-31 实施

江苏省市场监督管理局 发布
中国标准出版社 出版

目 次

前言 I

1 范围 1

2 规范性引用文件 1

3 术语和定义、缩略语..... 1

4 技术路线 2

5 部署要求 3

6 功能要求 3

 6.1 支持协议 3

 6.2 策略配置 3

 6.3 资产探测 3

 6.4 扫描分析 3

 6.5 监测及输出 5

7 性能要求 5

8 安全要求 5

 8.1 账户安全 5

 8.2 日志与审计 5

9 管理要求 5

 9.1 版本管理 5

 9.2 系统更新 5

 9.3 文档管理 6

附录 A（资料性） 视频监控联网信息安全自动化漏洞扫描报告模板 7

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由江苏省软件工程标准化技术委员会提出并归口。

本文件起草单位：南京市产品质量监督检验院（南京市质量发展与先进技术应用研究院）、南京治煜信息科技有限公司、国网电力科学研究院有限公司、东南大学、江苏苏测检测认证有限公司、南京虎牙信息科技有限公司、江苏省检验检疫科学技术研究院、公安部第三研究所、中国科学院信息工程研究所、中国工业互联网研究院、中国信息通信研究院、上海电器科学研究所（集团）有限公司。

本文件主要起草人：荣鼎慧、张小飞、朱嘉慧、张涛、王骥、王亚春、马鲜艳、宋宇波、唐雯、王晓、李盟、陈晶、童沐雨、裴世超、王蕊、季凯、李海洲、郭梦伊、王凯、徐一鸣、王尧、沈亮、孙永清、戚臻彦、闫兆腾、薛强、张志兵、任悦。

视频监控联网信息安全 自动化漏洞扫描技术规范

1 范围

本文件规定了视频监控联网信息安全自动化漏洞扫描技术规范,包括技术路线、部署要求、功能要求、性能要求、安全要求和管理要求。

本文件适用于视频监控联网设备、网络信息安全测试,包括但不限于智慧交通、城市安全、公共卫生及家庭生活等视频监控联网信息安全的自动化漏洞扫描。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

- GB/T 5271.1—2000 信息技术 词汇 第1部分:基本术语
- GB/T 37954—2019 信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法
- YD/T 3463—2019 漏洞扫描系统通用技术要求
- YD/T 3492—2019 视频监控系统网络安全技术要求

3 术语和定义、缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

漏洞 vulnerability

资产中能被威胁所利用的弱点。

[来源:GB/T 37954—2019,3.1]

3.1.2

漏洞扫描系统 vulnerability scanning system

一种针对安全漏洞开展主动检测的系统,可依据一定的策略,对目标系统进行安全漏洞的扫描,发现安全漏洞、验证安全漏洞并提出相应的改进意见。

[来源:YD/T 3463—2019,2.1.1]

3.1.3

视频监控系统 video surveillance system

由前端采集、传输、存储、管理、显示等组成,利用视频技术探测、监视设防区域并实时显示、记录现场图像的电子系统或网络。

[来源:YD/T 3492—2019,3.1.1]

3.1.4

固件 firmware

功能上独立于主存储器,通常存储在只读存储器(ROM)中的指令和相关数据的有序集。

[来源:GB/T 5271.1—2000,01.01.09]

3.1.5

可视化 visualization

利用计算机图形学和图像处理技术,将数据转换成图形或图像在屏幕上显示出来,并进行交互处理的理论、方法和技术。

[来源:YD/T 3463—2019,2.1.4]

3.2 缩略语

下列缩略语适用于本文件。

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

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

CVE:公共漏洞和暴露(Common Vulnerabilities & Exposures)

DVR:数字式录像机(Digital Video Recorder)

NVR:网络视频录像机(Network Video Recorder)

4 技术路线

通过接入目标系统网络,提取视频监控设备信息,并行执行固件漏洞检测、网络协议漏洞检测、业务交互内容漏洞检测的三大检测内容,最终分析检测数据并输出可视化结果及漏洞扫描报告。技术路线图见图1。

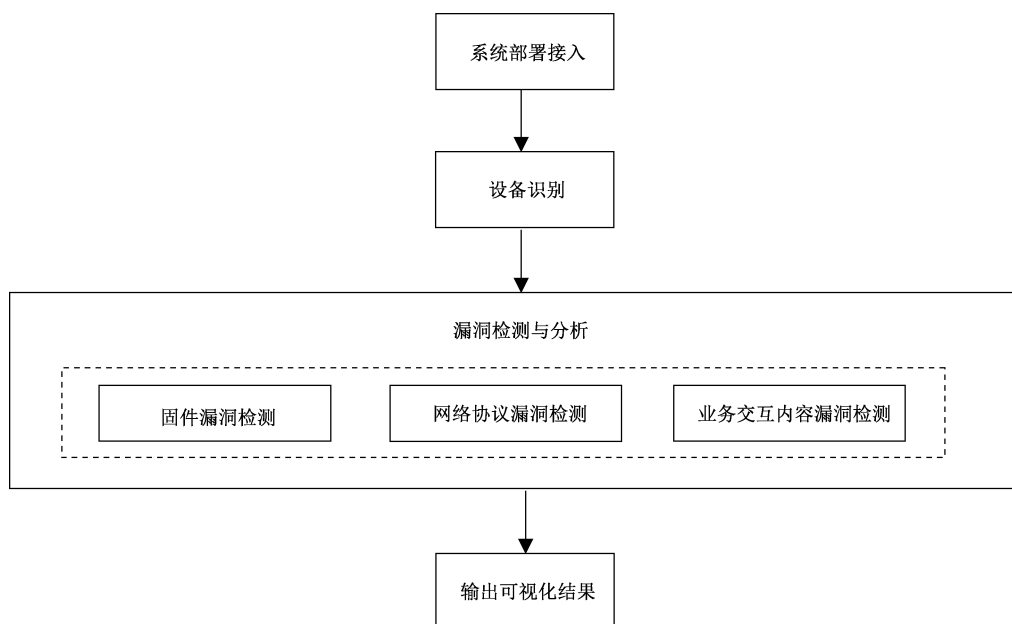


图1 技术路线图

5 部署要求

部署模式应符合 YD/T 3463—2019 第 3 章的要求。

6 功能要求

6.1 支持协议

支持协议类型包括 TCP/IP、UDP、RTSP、SOAP、UPNP、ONVIF 等。

6.2 策略配置

6.2.1 配置向导

扫描策略应支持可视化配置,包括但不限于以下内容:

- a) 任务信息的可视化,如任务名称、任务 ID 等;
- b) 扫描范围的可视化,如单一设备、多设备、多网段、连续 IP 节点等;
- c) 扫描周期的可视化,如仅一次、每周、每月或精确至具体时间等;
- d) 扫描方式的可视化,如全自动识别、人工增强等;
- e) 扫描目标的可视化,如摄像头设备、DVR/NVR、视频监控管理平台等。应支持针对常见厂商、架构的摄像头以及支撑摄像头运行的上下游设备做检测,做到对视频专网内设备的全覆盖。

注 1: 全自动识别指视频监控联网自动化漏洞扫描系统自动探测摄像头设备信息,并自动进行漏洞分析。

注 2: 人工增强指在系统自动探测的基础上,根据用户自主补充的摄像头设备信息,进行增强化的扫描与分析。

6.2.2 策略优化

扫描策略应支持结合摄像头指纹特征等信息进行调整,提升扫描效率及精确度。

6.3 资产探测

通过资产探测进行资产收集,资产信息收集应符合 YD/T 3463—2019 中 5.1.2 的规定。资产探测应形成视频监控设备信息表,包括但不限于以下内容:

- a) 视频监控设备基本信息:IP 信息、MAC 地址信息、厂商信息、版本号等;
- b) 视频监控设备扩展信息:协议信息、设备序列号、运行特征、端口号、Web 信息、组件版本等。

6.4 扫描分析

6.4.1 扫描规则

漏洞扫描规则基于漏洞数据库,漏洞数据库应包括 CVE、CNVD、CNNVD 等主流安全漏洞库,宜包括自主挖掘与收集的漏洞。

6.4.2 状态监测

视频监控联网自动化漏洞扫描系统每次发送检测数据包前,应对视频监控联网系统的性能状态与响应情况进行监测,如:网络性能压力、响应状态码、响应报文特征等。目标系统状态异常时,应立即停止扫描,并同步报送预警信息至监控端。

6.4.3 固件漏洞检测

6.4.3.1 检测对象

固件漏洞检测对象为视频监控终端的二进制固件代码。

6.4.3.2 检测过程

通过自动化解包、虚拟化运行、特征匹配等对二进制固件代码进行检测。

6.4.3.3 检查点

检测固件相关文件信息,如:固件名称、固件大小、固件的文件系统类型、固件文件结构、固件架构、组件版本等。

对固件进行安全检测,通过固件逆向、虚拟化运行、漏洞特征分析、漏洞缓解措施检测等方法进行检测,分析固件代码的安全问题,如漏洞存在情况、漏洞分类、漏洞出现位置。

6.4.4 网络协议漏洞检测

6.4.4.1 检测对象

网络协议漏洞检测对象为视频监控终端与后端服务等传输过程的协议数据包,分析对象包括但不限于常见的视频监控典型协议,如 RTSP、SOAP、UPNP、ONVIF 等。

6.4.4.2 检测过程

检测视频监控指纹特征等信息,自动产生模糊测试脚本,执行对每个待测设备的注入测试。

6.4.4.3 检查点

检测网络协议的完整性、保密性、可用性。协议完整性漏洞包括:视频监控协议指令与功能重放攻击、访问控制与设备配置项篡改等。协议保密性漏洞包括:视频监控视频流越权读取、密钥信息泄露、设备参数信息非法获取等。协议可用性漏洞包括:视频监控设备拒绝服务、非法关机与重启等。

6.4.5 业务交互内容漏洞检测

6.4.5.1 检测对象

业务交互内容漏洞检测对象为视频监控 Web 服务(如 Apache、Tomcat 等)、视频监控 Web 服务所依赖的数据库存储服务(如 Mysql、Oracle、Redis、ClickHouse 等)、视频监控 Web 服务所依赖的中间件服务(如 Docker、ElasticSearch、Kafka 等)。

6.4.5.2 检测过程

通过漏洞规则匹配对视频监控 Web 服务、视频监控数据存储服务、视频监控应用服务所依赖的中间件进行安全检测。

6.4.5.3 检查点

分析视频监控 Web 服务、视频监控应用服务所依赖的数据库存储服务、视频监控应用服务所依赖的中间件的漏洞信息、漏洞存在情况、漏洞分类等,如 SQL 注入、跨站脚本攻击、任意文件上传等。

6.5 监测及输出

6.5.1 可视化监测

可视化监测应包括以下内容：

- a) 监测被测设备的运行结果。当发现被测设备出现拒绝服务或者溢出错误等问题时，立即记录相应的输入和输出信息；
- b) 监测视频监控终端状态，如：终端运行状态、终端网络状态等；
- c) 监测网内摄像头资产管理、摄像头漏洞扫描、扫描器及漏洞库状态等信息；
- d) 监测网内摄像头资产数、已扫描设备数以及总扫描次数；
- e) 监测网内各个设备的漏洞情况，如云图、漏洞触发率排行表等。

6.5.2 结果输出

结果输出应满足以下要求：

- a) 扫描结果应支持自动保存、历史详情查看、导出为结果报告；
- b) 同一资产的两次历史扫描结果应能够进行对比分析，确认历史漏洞是否修复；
- c) 扫描结果内容应包括详细的漏洞扫描信息，如主机信息、端口信息、协议信息、漏洞存在情况、漏洞分类、漏洞位置、漏洞检测与利用方式等；
- d) 结果报告导出格式应支持多种常见文件类型，如 PDF、DOC/DOCX、HTML 等；
- e) 结果报告应支持版式及内容自定义配置。报告模板参见附录 A。

7 性能要求

性能应符合 YD/T 3463—2019 第 6 章的要求，资产的并发扫描应满足：

- a) 支持最大并发扫描资产数不低于 100；
- b) 支持最大并发扫描线程数不低于 1 000。

8 安全要求

8.1 账户安全

账户安全应符合 YD/T 3463—2019 中 7.1.2 及 7.2.2 的要求。

8.2 日志与审计

日志与审计应符合 YD/T 3463—2019 中 7.3 的要求，且日志存储时间应不少于 180 d。

9 管理要求

9.1 版本管理

版本管理应符合 YD/T 3463—2019 中 8.1.1 的要求。

9.2 系统更新

系统应具有更新、升级产品和漏洞库的能力。

9.3 文档管理

文档管理应符合 YD/T 3463—2019 中 8.1.2 的规定及以下要求：

- a) 漏洞扫描报告结果应能进行人工审计；
- b) 用户文档应提供用户手册、操作手册、运维手册等文档，指导用户使用、管理和维护系统。

附 录 A
(资料性)

视频监控联网信息安全自动化漏洞扫描报告模板

视频监控联网信息安全自动化漏洞扫描报告模板示例见表 A.1。

表 A.1 视频监控联网信息安全自动化漏洞扫描报告

开始时间：						
结束时间：						
主机信息						
状态	IP	MAC	主机名	开放 TCP 端口号	开放 UDP 端口号	
漏洞信息—端口信息						
端口	协议	漏洞名称	检测策略	漏洞详情	组件及版本	附加信息
