ICS 13.310
CCS A 91

CSPIA

团 体 标 准

T/CSPIA 013–2025

公共安全视频联网应用
网络安全漏洞应急修复指南

Emergency remediation guide for cybersecurity vulnerability of video surveillance networking application for public security

2025-10-15 发布 2025-12-01 实施

中国安全防范产品行业协会 发布

目　　次

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。

本文件由中国安全防范产品行业协会提出并归口。

本文件起草单位：公安部第三研究所、北京天防安全科技有限公司、公安部第一研究所、杭州海康威视数字技术股份有限公司、中国科学院信息工程研究所。

本文件主要起草人：齐力、杨明、张永元、栗红梅、杨乐好、段伟恒、考其瑞、李畅、万里、闫雪、白稳平、朱颖、汤宁、胡超飞、冯韶辉。

公共安全视频联网应用 网络安全漏洞应急修复指南

1 范围

本文件提出了公共安全视频联网应用中对通过网络进行攻击的网络安全漏洞进行应急修复的原则、能力、漏洞类型和技术实现方法。

本文件适用于公共安全视频联网应用中对通过网络进行攻击的网络安全漏洞进行应急修复的技术指导。

本文件不适用于通过邻接、本地、物理进行攻击的网络安全漏洞的应急修复。

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 25069—2022 信息安全技术 术语

GB/T 28181—2022 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 28458—2020 信息安全技术 网络安全漏洞标识与描述规范

GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南

3 术语、定义和缩略语

3.1 术语和定义

GB/T 25069—2022、GB/T 28458—2020、GB/T 30279—2020界定的以及下列术语和定义适用于本文件。

3.1.1

网络安全漏洞 cybersecurity vulnerability

网络产品和服务在需求分析、设计、实现、配置、测试、运行、维护等过程，无意或有意产生的、有可能被利用的缺陷或薄弱点。

注：这些缺陷或薄弱环节以不同形式存在于网络产品和服务的各个层次和环节中，一旦被恶意主体所利用，就会对网络产品和服务的安全造成损害，从而影响其正常运行。

[来源：GB/T 28458-2020，3.1]

3.1.2

网络安全漏洞应急修复 emergency remediation of cybersecurity vulnerability

针对可通过网络进行攻击和利用的网络安全漏洞，在无原厂补丁修复、受条件制约无法使用原厂补丁修复等情况下，在保障受保护对象的系统稳定性、系统性能、网络性能、关联业务应用运行等正常的前提下，实现对漏洞攻击和漏洞利用行为进行识别和有效控制的一种安全防护方法。

3.1.3

虚拟补丁 virtual patching

通过控制受保护对象的网络输入或输出，来防止对受保护对象的网络安全漏洞进行扫描、攻击、利用等行为的技术方法。

3.2 缩略语

下列缩略语适用于本文件。

DVR：数据视频录像机（Digital Video Recorder）
DVS：数字视频服务器 (Digital Video Server)
EXP：漏洞利用（Exploit）
FTP：文件传输协议（File Transfer Protocol）
IPC：网络摄像机（Internet Protocol Camera)
NTP：网络时间协议（Network Time Protocol）
NVR：网络硬盘录像机（Network Video Recorder）
ONVIF：开放式网络视频接口论坛（Open Network Video Interface Forum）
POC：概念验证(Proof of Concept)
RDP：远程桌面协议（Remote Desktop Protocol）
RTP：实时传输协议（Real-time Transport Protocol）
RTSP：实时流化协议（Real Time Streaming Protocol）
SIP：会话初始协议（Session Initiation Protocol）
SSH：安全外壳协议（Secure Shell）
VMS：视频管理系统（Video Management System)

4 网络安全漏洞应急修复原则

网络安全漏洞应急修复宜遵循以下原则：

a) 网络安全漏洞应急修复对受保护对象的运行性能产生较小影响；
b) 能识别和防护加密和非加密网络通讯场景下对网络安全漏洞的扫描、攻击及利用等行为；
c) 优先修复等级为超危、高危、中危等的网络安全漏洞。

5 应急修复网络安全漏洞类型

可应急修复的网络安全漏洞包括但不限于以下类型：

a) 前端设备（IPC、NVR、DVR等）、视频应用服务器（DVS、VMS、媒体服务器、中心信令服务器、视频存储服务器等）的网络安全漏洞；
b) 视频应用协议（GB/T 28181协议、GA/T 1400协议、SIP、RTSP、RTP等）相关的网络安全漏洞；
c) 公共安全视频联网应用中常见应用（FTP、TELNET、SSH、RDP、NTP等）、数据库（Mysql、Elasticsearch、Redis等）、中间件（Zookeeper、WebLogic、Log4j等）相关的网络安全漏洞。

6 网络安全漏洞应急修复能力

在网络安全漏洞无实质修复前，在不影响用户业务正常运行前提下，网络安全漏洞应急修复宜提供以下能力：

a） 提供对加密和非加密场景下网络通讯中基于POC的漏洞扫描行为进行识别和防护能力；
b） 提供对加密和非加密场景下网络通讯中基于EXP的漏洞攻击及利用行为进行识别和防护能力；
c） 提供对非加密网络通讯中基于版本匹配的漏洞扫描行为进行识别和防护能力；
d） 提供的可应急修复的网络安全漏洞数量建议不低于400个，分级等级为中危、高危及以上的漏洞占比建议不低于70%；
e） 针对受保护对象增加的网络延时上限建议不超过400ms。

7 应急修复技术实现

7.1 基于网关技术的网络安全漏洞应急修复

7.1.1 修复方法

在受保护对象的网络接入位置部署基于虚拟补丁技术实现的专用网关设备，对流经网关设备的数据流进行分析，识别视频网络中针对受保护对象的网络安全漏洞的漏洞检测、漏洞攻击和漏洞利用等行为,通过对上述行为的关联数据包进行拦截阻断或修改重组数据包的方法，使得漏洞检测、漏洞攻击和漏洞利用等行为无法继续进行，进而实现对受保护对象网络安全漏洞的应急修复。

7.1.2 修复流程

基于网关技术实现的应急修复工作流程见图1，包括：网络流量预处理、网络行为分析、网络漏洞应急修复。具体步骤如下：

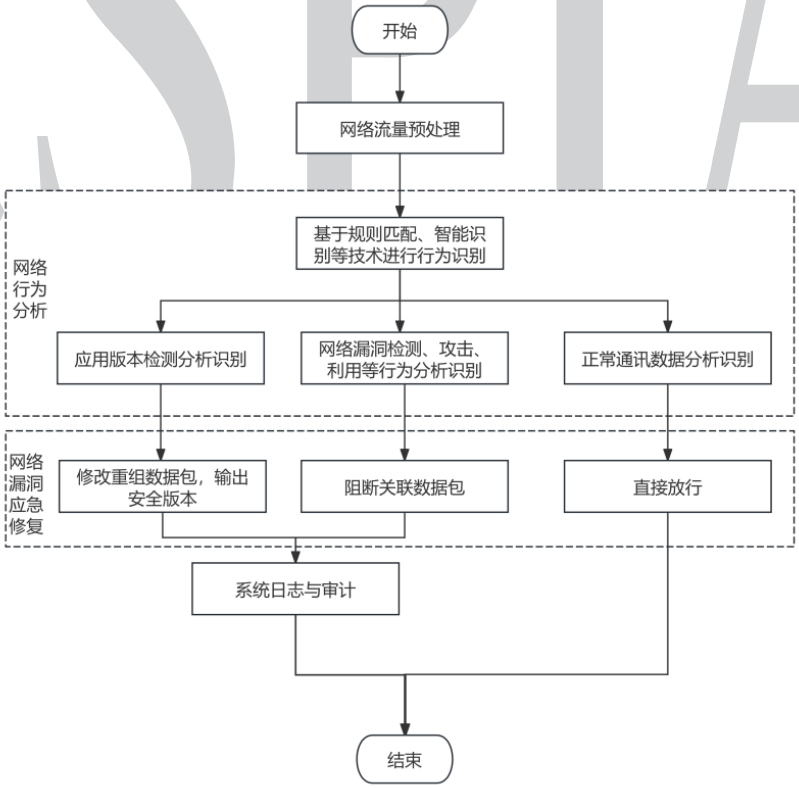

图 1 基于网关技术的应急修复工作流程图

a) 网络流量预处理：通过网络抓包的方式对流经网关的网络流量进行捕获，并对网络流量进行传输层和应用层的协议解析和识别；
b) 网络行为分析：根据网络流量预处理的结果，利用规则匹配及智能识别等技术对网络流量中的应用版本检测、网络漏洞检测、漏洞攻击、漏洞利用行为进行识别；
c) 网络漏洞应急修复：根据网络行为分析的检测结果，对于应用版本检测行为，针对存在安全问题的应用版本，采用修改重组数据包替换原有版本的方法，输出对应应用的安全版本，防止基于版本检测的漏洞扫描；对于网络漏洞检测、漏洞攻击、漏洞利用等行为，采用TCP RST或直接丢弃数据包等方法阻断关联数据包中断其网络通讯，保护设备及应用安全；对于正常通讯数据，则直接放行；
d) 系统日志与审计：针对重组数据包和阻断关联数据包的行为，建议进行相应的日志记录和行为审计，为日后跟踪和分析系统运行状态提供依据。

7.1.3 自身安全保障

实施修复的网关设备宜满足以下自身安全要求：
a) 设备操作系统进行内核精简和安全加固，采用最小化服务原则，保证设备自身安全性；
b) 对设备进行自身信息安全检测或评估，保证设备自身安全性；
c) 支持设备冗余和系统备份。

7.1.4 部署模式

实施修复的网关设备宜满足以下要求：
a) 可通过串接、策略路由或旁路方式部署；
b) 串接部署方式部署位置尽量靠近受保护对象，以提供最优防护能力；
c) 串接部署方式考虑实际网络流量负载、自身网关处理能力等因素，不能对正常的网络通讯造成网络延迟显著增加等不利影响；
d) 串接部署方式支持bypass功能，防止出现设备故障造成的网络中断，防止单点故障；
e) 策略路由部署方式在部署前与用户进行充分沟通，对路由做好统一规划，防止出现因路由改变所导致的网络故障；
f) 旁路部署方式应充分考虑网络流量负载、自身处理能力等因素。

7.2 基于客户端代理技术的网络安全漏洞应急修复

7.2.1 修复方法

在受保护对象操作系统中安装基于虚拟补丁技术实现的客户端代理程序，通过客户端代理程序对受保护对象本地网卡的数据流进行分析、识别网络中针对受保护对象的网络安全漏洞的漏洞检测、漏洞攻击和漏洞利用等行为，并通过对上述行为的关联数据包进行拦截阻断或修改重组数据包的方法，使得漏洞检测、漏洞攻击和漏洞利用等行为无法继续进行，进而实现对受保护对象网络安全漏洞的应急修复。

7.2.2 修复流程

基于客户端代理技术实现的应急修复工作流程见图2，包括：本地网卡流量预处理、网络行为分析、网络漏洞应急修复。具体步骤如下：

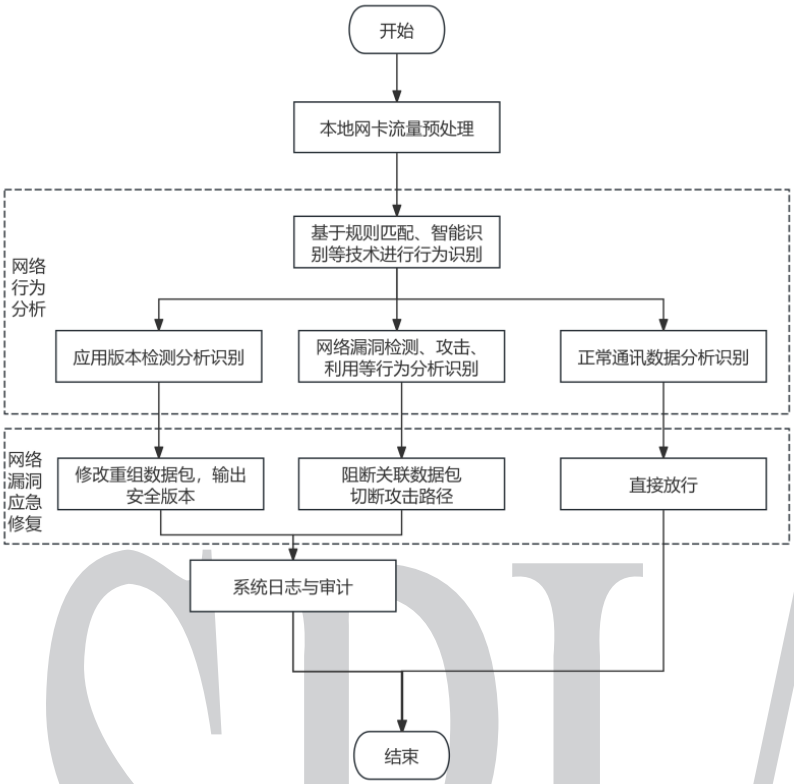

图 2 基于客户端代理的应急修复工作流程图

a) 本地网卡流量预处理：通过网络抓包方式对本地网卡的网络流量进行捕获，并对网络流量进行传输层和应用层的协议解析和识别；
b) 网络行为分析：根据网络流量预处理的结果，对网络流量中的应用版本检测、网络漏洞检测、漏洞攻击、漏洞利用行为进行识别；
c) 网络漏洞应急修复：根据网络行为分析的检测结果，对于应用版本检测行为，针对存在安全问题的应用版本，采用修改重组数据包替换原有版本的方法，输出对应应用的安全版本，防止基于版本检测的漏洞扫描；对于网络漏洞检测、漏洞攻击、漏洞利用等行为，采用TCP RST或直接丢弃数据包等方法阻断关联数据包中断其网络通讯，清除漏洞利用前置文件切断漏洞攻击路径；对于正常通讯数据，则直接放行；
d) 系统日志与审计：针对重组数据包和阻断关联数据包的行为，建议进行相应的日志记录和行为审计，为日后跟踪和分析系统运行状态提供依据。

7.2.3 自身安全保障

实施修复的客户端代理宜满足以下自身安全性要求：
a) 具备防止非授权用户强行终止客户端代理程序运行的措施；
b) 具备防止非授权用户强制取消客户端代理程序在系统启动时自动加载的措施；
c) 具备防止非授权用户强行卸载、删除或修改客户端代理程序的措施。

7.2.4 部署模式

客户端代理的部署宜满足以下要求：

a） 客户端代理程序具备良好的系统兼容性和稳定性，至少能够兼容Windows、Linux和国产化操作系统，提供客户端支持的详细操作系统列表；
b） 客户端代理程序具备应用兼容性，不与其他本地业务应用产生冲突；
c） 客户端代理程序支持集中管理、统一策略配置与分发能力、统一自动升级能力；
d） 提供对客户端代理程序非正常中断、卸载、离线等异常行为进行集中监测的机制。