HIKVISION

海康威视
外部安全报告处理流程

编写人	海康威视安全应急响应中心
版本号	1.2
最后更新日期	2021-12-15

目录

一、 文档说明

【适用范围】

本流程适用于海康威视安全应急响应中心（漏洞上报 – 安全应急响应中心 – 海康威视 Hikvision）安全报告处理流程。

【实行日期】

自 2021 年 12 月 15 日起实行。

二、 基本原则

1. 海康威视非常重视自身产品和业务的安全问题，我们希望通过外部安全专家提交漏洞的方式提升业务安全，从而保障用户的信息安全。我们承诺：每一份安全报告问题都会有专人进行评估、分析，并及时反馈最新处理进展。
2. 海康威视支持负责任的漏洞披露和处理过程，我们承诺：对于每位保护用户利益，帮助海康威视提升安全质量的用户，我们将给予感谢和回馈。
3. 海康威视反对和谴责一切以漏洞测试为借口，利用安全漏洞进行破坏、损害用户利益的黑客行为，包括但不限于利用漏洞盗取用户隐私及虚拟财产、入侵业务系统、非授权获取系统（业务）数据、窃取用户数据、恶意传播漏洞或数据等。 未经允许请勿在任何公众场合或平台讨论或披露产品漏洞或情报细节。如有上述行为，海康威视有追究其法律责任。
4. 《中华人民共和国网络安全法》、《网络产品安全漏洞管理规定》已正式实施。我们呼吁白帽子们遵守相关规定，规避不必要的法律风险。
5. 海康威视认为每个安全漏洞的处理与整个安全行业的进步，都离不开各方的共同合作。海康威视希望加强与业界企业、安全公司、安全研究者的合作，共同维护行业信息安全。

三、 安全漏洞处理流程

【漏洞提交】

漏洞报告者发送邮件至 HSRC@hikvision.com 来报告您所发现的安全漏洞。

【漏洞审核阶段】

1. 两个工作日内，海康威视安全应急响应中心（Hikvision Security Response Center，以下简称 HSRC）工作人员会确认收到漏洞报告并跟进开始评估问题。
2. 五个工作日内，HSRC 工作人员处理问题、给出结论。必要时会与报告者沟通确认，请报告者予以协助。

【漏洞处理阶段】

业务部门修复漏洞，修复时间根据问题的严重程度及修复难度而定。部分漏洞受版本发布限制，修复时间根据实际情况确定。严重或重大影响漏洞会单独发布紧急安全公告。

四、 通用漏洞评估标准

根据漏洞危害程度分为严重、高危、 中危、低危、忽略五个等级，每个等级评估如下：

【严重】

1. 直接获取核心系统权限（服务器端权限、客户端权限）的权限。包括但不限于：命令注入、远程命令执行、上传获取 WebShell、SQL 注入获取系统权限、远程内核代码执行漏洞以及其它因逻辑问题导致的远程代码执行漏洞。
2. 严重的逻辑设计缺陷。包括但不仅限于关键业务系统的任意账号登陆、任意账号密码修改、任意账号资金消费、订单遍历、交易支付方面的严重问题。
3. 严重级别的信息泄漏。包括但不限于通过 SQL 注入、接口越权等方式获取海量敏感信数据多元组或大量重要数据库信息。

【高危】

1. 能直接盗取用户身份信息的漏洞。包括重点页面的存储型 XSS 漏洞、普通站点的 SQL 注入漏洞。
2. 未授权访问。包括但不仅限于绕过认证直接访问管理后台、后台弱密码且后台存在实际重要业务信息或者个人敏感信息、篡改系统前端页面等。
3. 高风险的信息泄漏漏洞。包括但不限于源代码压缩包泄漏。
4. 高风险的 SSRF，支持多种协议，可探测内网服务并窃取内网重要信息或者可拿到内网服务器权限的漏洞。
5. 高风险的逻辑设计缺陷。如认证模块的短信验证码绕过、邮件验证绕过、短信验证码暴力破解，可造成任意用户登录或密码重置。

【中危】

1. 需交互才能获取用户身份信息的漏洞。包括但不限于反射型 XSS（包括反射型 DOM-XSS）、可成功利用并窃取用户重要信息或权限的 CSRF、普通业务的存储型 XSS。
2. 普通信息泄漏漏洞。包括但不限于包含敏感信息（如数据库连接密码）的压缩包泄漏。
3. 普通越权操作。包括但不仅限于不正确的直接对象引用。
4. 普通逻辑设计缺陷。包括但不仅限于非认证模块的短信验证码绕过、邮件验证绕过、短信验证码暴力破解。

5. 非关键业务、利用难度较大的 SQL 注入漏洞等。

【低危】

1. 轻微信息泄漏漏洞。包括但不限于路径泄漏、SVN 信息泄漏、LOG 文件泄露、正确的内网账号密码、GitHub 泄露的非敏感系统源码及密码等。
2. 难以利用但又可能存在安全隐患的问题。包括但不限于可能引起传播和利用的 Self-XSS、文件解析漏洞、客户端密码明文传输（仅限使用 http 的站点）、注销后凭证不失效。
3. 拒绝服务漏洞。如不需要大量资源就可造成网站拒绝服务的漏洞。
4. 普通的运维管理系统、测试数据库等未授权访问，没有重要数据或者其他进一步利用的情况。

【忽略】

1. 无实际危害的问题。包括但不仅限于产品功能缺陷、页面乱码、样式混乱、不泄露敏感信息的报错不能重现的漏洞。
2. 无法利用或者没有利用价值的漏洞。包括但不仅限于无意义的目录遍历、401 基础认证钓鱼、有编码缺陷但无法利用的问题、Self-XSS、无敏感操作的 CSRF、无意义的异常信息泄露/前端源码泄露、无实际危害证明的扫描器结果、无敏感信息的 json hijacking、仅有 js 与 img 等的打包文件、一般信息的 logcat、用户名明文传输、iframe 嵌套钓鱼、未实现 SSL/TLS 最佳安全实践等。
3. 不能直接体现漏洞的其他问题。包括但不仅限于纯属用户猜测的问题、不包含敏感信息的测试页面等。SSRF 漏洞无法获取内网的相关服务器信息，仅简单访问 dnslog，无任何其他影响的问题。仅说明理论可行无实际利用案例的、使用了有漏洞的库但无法直接利用、未使用最佳安全配置等。
4. 非核心客户端本地拒绝服务漏洞，包括但不仅限于组件参数未验证导致的拒绝服务漏洞。普通的运维管理系统等未授权访问，没有数据或者其他可利用的地方。无实际影响的 slowhttptest。需要较大成本的 ddos 攻击。Web 端的中间人劫持类问题。第三方工具或在线平台的扫描结果不能直接作为漏洞证明，无法提供具体的漏洞描述、验证方式和危害的，仅报告站点使用 HTTP 协议而非 HTTPS 协议不被认为是安全问题。仅报告端口开放而无法提供利用手段，如开放 MySQL 服务等。无法再次复现的漏洞。
5. 违反安全设计原则但无法给出利用手段的，如密码策略。可爆破账号密码，但是未成

功爆破出账号密码的。静态文件存储的 pdfxss，百度地图 ak 信息,actuator 无实际影响的开放路径如 prometheus、并发点赞、并发少量短信等

6. 非关键业务系统且影响范围不大的账户问题，包括但不限于用户名及手机号枚举、僵尸用户注册、图片验证码失效、撞库、口令暴力破解、邮件轰炸、短信轰炸等。包括但不仅限于经 HSRC 专员确认无法重现的漏洞。

五、 IoT 漏洞评估标准

根据漏洞危害程度分为严重、高危、 中危、低危、忽略五个等级，每个等级评估如下：

【严重】

1. 无交互远程命令执行、任意代码执行等能导致远程控制设备并且窃取设备内隐私信息的漏洞。
2. 远程导致设备永久性拒绝服务的漏洞。包括但不仅限于系统设备遭到远程发起的永久性拒绝服务攻击（设备无法再使用：完全永久性损坏，或需要重新刷写整个操作系统）。

   注：需要提供 exp 或者能够证明漏洞可用性的 poc。

【高危】

1. 远程获取系统非特权权限的漏洞。包括但不仅限于远程命令执行、任意代码执行等漏洞。局域网内的无交互命令执行,能够获取设备内隐私信息的漏洞。

   注：需要提供 exp 或者能够证明漏洞可用性的 poc。
2. 导致设备拒绝服务的漏洞。包括但不仅限于系统设备遭到本地发起的永久性拒绝服务攻击（设备无法再使用：完全永久性损坏，或需要重新刷写整个操作系统）、远程攻击导致的暂时性拒绝服务攻击漏洞（远程挂起或者重新启动）。
3. 远程越权操作漏洞。包括但不仅限于远程绕过需要用户发起或者获得用户许可后方可使用的功能限制，进行越权敏感操作的漏洞。
4. 权限绕过漏洞。包括但不仅限于全面深入的绕过内核级防护功能，或利用缓解技术存在的漏洞、本地绕过针对用户功能要求限制对任何开发者或针对任何安全设置进行修改、全面绕过应用隔离操作系统保护功能。
5. 本地获得系统特权权限的漏洞。包括但不限于本地权限提升漏洞。

【中危】

1. 局域网内的有交互或者授权后命令执行，需要较苛刻环境下才能触发的危害较高的漏洞。
2. 导致设备暂时性拒绝服务攻击漏洞，包括但不仅限于本地攻击导致的暂时性拒绝服务攻击漏洞。
3. 权限绕过漏洞。包括但不仅限于全面深入的绕过用户级防护功能，或在特权进程中利用缓解技术存在的漏洞、绕过设备保护功能的漏洞。

4. 本地越权操作漏洞。包括但不仅限于本地绕过需要用户发起或者获得用户许可后方可使用的功能限制，进行越权敏感操作的漏洞。
5. 远程越权访问非敏感受控数据的漏洞。

【低危】

1. 不安全配置（利用难度较大或无较大影响的问题将忽略）低危的信息泄露需要物理接触，危害只造成信息泄露或有安全风险类漏洞；局域网内的拒绝服务、需用户交互后才能利用的拒绝服务。
2. 权限绕过漏洞。包括但不仅限于全面深入的绕过用户级防护功能，或在非特权进程中利用缓解技术存在的漏洞、本地绕过系统权限控制获取用户的非敏感受控数据的漏洞。
3. 本地越权操作漏洞。包括但不仅限于不通过用户交互的情况下，调用系统隐藏功能，对用户的使用造成实际困扰或发生实际损失的漏洞。

【忽略】

1. 低影响拒绝服务：没有安全影响的软件功能性错误、应用程序级别的崩溃、简单的提示性弹窗、临时性的 Framework 重启；
2. 缺少证书绑定；受 TLS 保护下的 URL/请求报文中敏感数据传输；
3. 普通权限 APP 无法访问到的敏感信息存储；对用户无实际影响的日志数据、系统测试数据等；
4. 用户数据未经加密存储于外部存储设备中(带有敏感信息的 APP 日志以及已经承诺了加密存储的用户数据除外)；
5. APP 缺少代码混淆保护，APK 可以被重打包，APP 中含有硬编码或可恢复的密钥，APP 中缺乏二进制保护控制；
6. 通过物理接触，破坏设备硬件完整性才可以发起的攻击；
7. 在开发者模式下发起的攻击（影响较大的可例外评估，如提权漏洞）；
8. 同时影响其他业界设备的开源及第三方漏洞（对设备影响较大的漏洞可例外评估）；
9. 当涉及的漏洞需要依赖某些权限才可被成功利用并造成影响，而该权限本身就可以造成同样效果，这样的情况我们不会进行奖励；
10. 只是提到存在漏洞的可能性但未提及利用方式，或者是无实际危害证明的扫描器结果，以及基于非法获得的机密信息所做的漏洞报告。

【评估标准通用原则】

1. 评估标准仅针对海康威视产品和业务。域名包括但不限于 www.hikvision.com、www.hikyun.com、www.hikmall.com、www.hik-cloud.com、www.hiklink.cn 等，产品为海康威视发布的产品或解决方案。与海康威视完全无关的漏洞，无奖励。
2. 由同一个漏洞源产生的多个漏洞计漏洞数量为一个，例如；服务器某一配置、应用框架某一全局功能、同一文件或模板、泛域名解析等引起的多个问题。
3. 在上报漏洞之前，该漏洞的技术细节（如：POC 等信息）已经公开，包括但不限于网站、自媒体、邮件组、公开演讲、即时聊天群等，此类漏洞无法参与漏洞奖励计划；
4. 多人或同一人提交重复的漏洞场景/同样的漏洞成因，第一个提交的漏洞报告被视为有效，其他被视为不符合资格；由于硬件、系统及架构相关漏洞修复发版周期较长，相关漏洞（含 nday 漏洞）重新收取的时间以内部安全工单修复完成时间为准。
5. 非关键业务系统网站漏洞，视漏洞影响范围评级酌情降低。反之，关键业务系统且影响范围较大的漏洞，评级酌情提高。
6. 以漏洞测试为借口，利用漏洞进行损害用户利益、影响业务正常运作、修复前公开、盗取用户数据等行为的，将无奖励，同时海康威视保留采取进一步法律行动的权利。

六、 争议解决办法

在漏洞处理过程中,如果报告者对处理流程、漏洞评定、漏洞评分等具有异议的 ,请通过邮件： HSRC@hikvision.com 并以邮件标题【海康威视漏洞处理异议】 进行反馈，我们会有专门工作人员负责优先处理此类反馈。HSRC 将按照漏洞报告者利益优先的原则处理，必要时可引入外部安全人士共同裁定。

七、 奖励制度

对于提交高质量漏洞或者非常积极参与活动的外部安全专家，我们会不定期给予特别奖励。 如因收件人信息未及时完善或错误、快递公司问题及不可抗拒因素产生的礼品丢失，HSRC 不承担责任。