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	**1.1**
最后更新日期	**2017-09-11**

目录

一、 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，我们承诺，对每一位报告者反馈的问题都有专人进行跟进、分析和处理，并及时给予答复。

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。

4) 《中华人民共和国网络安全法》于 2017 年 6 月 1 日正式实施。我们呼吁白帽子们遵守网络安全法中的相关规定，规避不必要的法律风险。《中华人民共和国网络安全法》的地址是：http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm。

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。

二、 漏洞反馈与处理流程

【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) 一个工作日内，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) 三个工作日内，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。

【修复&完成阶段】

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， 严重和高风险漏洞 24 小时内，中危风险三个工作日内，低危风险七个工作日内。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。

三、 安全漏洞评估标准

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) 直接获取系统权限(服务器端权限、客户端权限)的漏洞。包括但不仅限于 :命令注入、远程命令执行、上传获取 WebShell、SQL 注入获取系统权限、缓冲区溢出（包括可利用的 ActiveX 缓冲区溢出 ）、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 。包括但不限于重要 DB 的 SQL 注入漏洞，可获取大量核心用户的身份信息、订单信息、银行卡信息等接口问题引起的敏感信息泄露。

【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) 越权访问。包括但不仅限于绕过认证直接访问管理后台、后台弱密码。

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) 直接获取移动客户端权限。包括但不仅限于远程命令执行、任意代码执行。

【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）、重要敏感操作的 CSRF、普通业务的存储型 XSS。

2) 本地应用拒绝服务漏洞（包括一些较难利用的客户端漏洞）、敏感信息泄露、内核拒绝服务漏洞、可获取敏感信息或者执行敏感操作的 XSS 漏洞。

3) 普通信息泄漏漏洞。包括但不限于客户端明文存储密码、包含敏感信息（如 DB 连接密码）的压缩包泄漏。

4) 普通越权操作。包括但不仅限于不正确的直接对象引用。

5) 普通逻辑设计缺陷。包括但不仅限于短信验证码绕过、邮件验证绕过、短信无限制发送。

6) 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、Phpinfo 等。

2) 移动客户端本地拒绝服务漏洞。包括但不限于组件权限导致的本地拒绝服务漏洞。

3) URL 跳转。包括但不仅限于未验证的重定向和转发。

4) 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。

5) 只在特定非流行浏览器环境下（如 IE6 等）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）、普通业务的存储型 XSS 等。

【忽略】

1) 无关安全的 bug。包括但不限于网页乱码、产品功能缺陷、样式混乱。
2) 无法利用的“漏洞”。包括但不限于没有实际意义的扫描器漏洞报告（如 Web Server 的低版本）、Self-XSS、无敏感信息的 JSON Hijacking、无敏感操作的 CSRF、无意义的异常信息泄露、内网 IP 地址/域名泄漏。
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。
4) 不能重现的漏洞。包括但不仅限于经 HSRC 专员确认无法重现的漏洞。
5) 非关键业务系统且影响范围不大的账户问题，包括但不限于垃圾用户注册、字典攻击引起的撞库等。

【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，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) 提交网上已公开的漏洞无奖励。
3) 非关键业务系统或已弃用的网站漏洞，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。
4) 同一漏洞最早提交者有奖励。
5) 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。
6) 同一份报告中提交多个漏洞，只按危害级别最高的漏洞评级。
7) 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。

四、 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。

五、 奖励制度

对于提交高质量漏洞或者非常积极参与活动的安全专家，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。

奖励处理细节最终解释权归海康威视安全应急响应中心所有。