360 安全应急响应中心

奇酷手机安全漏洞响应流程

北京奇虎科技有限公司

2015 年 11 月

Ver:1.2

文档信息

一般信息	细节
名称	奇酷手机安全漏洞响应流程
作者	白嘎力
贡献者	陈豪，张培德，宋申雷

文档版本控制

版本	日期	姓名	注释
1.0	2015.11.01	白嘎力	第一版
1.1	2015.11.05	白嘎力	更改漏洞评估标准，定级，分类漏洞类型
1.2	2015.11.13	白嘎力	更新调整远程利用漏洞奖金金额范围

版权申明

奇酷手机系统漏洞响应处理流程 V1.1

背景：

为了保障奇酷手机 OS 开发安全，360 安全团队协助奇酷在操作系统及应用开发上提供必要的安全性防范措施，全面提供漏洞的跟踪处理及预警等安全服务，确保安全漏洞在第一时间被修复，持续为奇酷手机用户提供一个安全的 android 手机操作系统环境。

现 360 安全应急响应中心（以下简称 360SRC）依托 360 安全响应中心（security.360.cn）平台负责收集奇酷手机 OS 安全漏洞。

此办法适用于奇酷手机 0S 漏洞响应、处理、修复、披露过程细则。

Google 官方将 chrome app 加入单独的 non-aosp 软件漏洞奖励计划。由于奇酷公司及 360 公司开发的预装应用用户可以自由卸载，奇酷手机参考业界标准，将部分预装应用列入单独奇酷 APP 漏洞奖励范围。

奇酷手机漏洞收集和奖励范围：

1.奇酷手机应用/APP 漏洞：奇酷公司及 360 公司开发的预装应用、非 aosp 系统服务

2.奇酷手机系统/OS 漏洞：AOSP 系统服务，预装系统应用，MTK 驱动漏洞（含未公开）

一、漏洞响应

360SRC 收集奇酷手机漏洞同时第一时间评估威胁等级，提供修复解决方案。

二、漏洞处理

收到安全漏洞后产品团队按照安全专家建议进行修复工作。

其中对解决方案有异议可进行沟通解决，确保产品不影响产品正常使用的情况下，依照用户体验角度进行适当的调整。

三、漏洞修复周期

对于高危安全漏洞，第一时间响应处理，漏洞修复后将第一时间更新

对于中危安全漏洞，漏洞修复后第一时间更新更新或并入特定版本集中修复。

对于低危安全漏洞，按照正常发布流程，并入特定版本集中修复

四、漏洞披露

360 对安全漏洞负责任对外披露原则，对外不公开具体漏洞细节，但披露漏洞修复进度，漏洞版本号及致谢等。

五、安全漏洞评估标准

按照漏洞攻击导致的后果和威胁程度评级漏洞，分为严重，高危，中危，低危级别。

按照漏洞利用方式：远程，本地，中间人劫持，拒绝服务四种类别。

远程利用漏洞评级

包括但不仅限于通过网页渲染，网络连接，远程协议连接等远程利用场景，产生的代码执行，命令执行等漏洞危害。

严重：5000 -10000

超出原有功能，没有交互，无感知静默执行

高危：3000 - 5000

超出原有功能，有交互，有感知静默执行

中危：1500 - 3000

在原有功能上实现，静默或者无感知执行

低危：500 - 1500

在原有功能上实现，有交互，有感知执行

本地利用漏洞评级

包括但不仅限于通过物理接触，本地安装 app 等本地利用场景，产生的越权，代码执行，命令执行等漏洞危害。

严重：3000 - 5000

超出原有功能，没有交互，无感知静默执行

高危：1500 - 3000

超出原有功能，有交互，有感知静默执行

中危：1000 - 1500

在原有功能上实现，静默或者无感知执行

低危：100 - 500

在原有功能上实现，有交互，有感知执行

中间人劫持漏洞评级

在不安全网络或者用户不可控的网络环境中受到的中间人攻击

严重：3000 - 5000

无任何条件限制，包括但不限于中间人劫持修改了一个攻击载体，如篡改一个网页导致代码执行等，造成代码执行，命令执行或静默安装 apk 等漏洞危害。

高危：1500 - 3000

需要一定条件触发，如攻击者可控或可提高攻击成功率的攻击条件，无交互过程，造成代码执行，命令执行或静默安装 apk 等漏洞危害。

中危：1000 - 1500

需要被动触发条件，如后台常驻服务开启和特定 APP 开启等条件，造成代码执行，命令执行或静默安装 apk 等漏洞危害。

低危：100 - 500

需要交互触发条件，具有明显交互界面，弹窗提示，需要人工点击等条件 ，造成代码执行，命令执行或静默安装 apk 等漏洞危害。

拒绝服务漏洞和其他特殊类漏洞评级

1. 拒绝服务漏洞，只接受在特定场景下，针对系统常驻服务或系统底层驱动攻击，造成手机假死或重启情况。其他不列入安全漏洞范围，按程序普通 BUG 处理。
2. 其他涉及软件逻辑、信息泄露、安全功能绕过等特殊类安全问题，需官方评估后定级。