

2019 年上半年度

# 安卓系统安全性生态环境 研究



**360 互联网安全中心**

2019 年 8 月 13 日

## 摘 要

- ✧ 此报告数据来源为“360 透视镜”（360 团队发布的一款专业检测手机安全漏洞的 APP, <http://shouji.360.cn/vulscanner.htm>）用户主动上传的 62 万份漏洞检测报告，检测内容包括最近两年的 Android 和 Chrome 安全公告中检出率最高的 104 个漏洞，涵盖了 Android 系统的各个层面。
- ✧ 检测结果显示，截止至 2019 年 8 月，所测设备中 99.97% 的 Android 手机存在安全漏洞，仅有 0.03% 的设备完全没有检测出漏洞，同比 2018 年，手机安全程度呈上升趋势。
- ✧ Android 版本占比最高的 3 个版本分别为 Android 6.0、Android 5.1 和 Android 7.1，比例分别为 37%、23% 和 19%。与 2018 年相比，用户整体的版本更新有所推进，低版本系统 5.1 和 4.4 数量不断减少，Android 8.0 和 8.1 数量持续在上升，最新的 Android 9.0 版本占比也达到了 2%。从漏洞分布上看，Android 版本高低和漏洞数量多少并没有严格的线性关系，由于 Google 目前只对 7.0 及以上系统提供安全更新，所以在高版本系统（7.0 及以上版本）上，漏洞数量明显减少。
- ✧ 用户手机的平均漏洞数量存在比较明显的地域特征，安徽、北京、上海等地区的用户手机平均漏洞数量最少，黑龙江、宁夏、西藏等地区的用户手机漏洞数量相对较多。大致上，经济越发达的地区，用户所使用的手机的平均漏洞数量越少，手机安全程度相对越高。
- ✧ 不同性别的用户平均系统版本较 2018 年均有所提升，同时不同性别的用户漏洞平均漏洞数量也有所下降。女性用户的手机系统版本提升幅度高于男性用户，男性用户的手机平均漏洞数量略高于女性用户。
- ✧ 其中 99.4% 的设备存在浏览器内核相关漏洞，浏览器内核漏洞最多的设备同时存在 7 个漏洞，有半数以上的设备浏览器内核漏洞数达到 3 个以上，仅有 0.6% 的设备不受浏览器内核漏洞影响。
- ✧ 安卓手机用户中，约有 45.2% 的用户会保持手机系统（特指安全补丁等级）版本与厂商所提供的最新版本保持一致，约有 11.7% 的用户的手机系统版本会滞后厂商最新版本 1 到 3 个月，接近 5.9% 的用户会滞后 4 到 6 个月，其余用户会滞后半年以上。
- ✧ 与安卓官方最新更新情况相比，与安卓官方更新保持同步的手机仅占 2.8%，滞后一年以上的手机占 63.5%。由此可见，用户手机因未能及时更新而存在安全漏洞的重要原因之一，就是手机厂商定制开发的安卓系统普遍未能与 Google 官方同步更新，而且滞后性比较明显。

**关键词：**安卓安全、安卓漏洞、漏洞检测

# 目 录

|                                   |           |
|-----------------------------------|-----------|
| 研究背景 .....                        | 1         |
| <b>第一章 手机系统安全性综述 .....</b>        | <b>1</b>  |
| 一、 系统漏洞的危险等级 .....                | 1         |
| 二、 系统漏洞的危害方式 .....                | 1         |
| 三、 系统浏览器内核的安全性 .....              | 3         |
| 四、 系统漏洞的数量分布 .....                | 5         |
| 五、 手机安全生态宏观描述 .....               | 6         |
| <b>第二章 手机系统版本安全性 .....</b>        | <b>8</b>  |
| 一、 各系统版本漏洞情况 .....                | 8         |
| 二、 安卓系统漏洞缓解措施 .....               | 9         |
| <b>第三章 手机系统安全性地域分布 .....</b>      | <b>11</b> |
| <b>第四章 手机系统安全性与用户性别的相关性 .....</b> | <b>13</b> |
| <b>第五章 手机系统安全漏洞的修复 .....</b>      | <b>15</b> |
| 一、 厂商漏洞修复情况 .....                 | 15        |
| 二、 用户主动升级意愿 .....                 | 15        |
| 三、 漏洞修复综合分析 .....                 | 17        |
| <b>第六章 新品手机安全更新情况 .....</b>       | <b>18</b> |
| 附录 .....                          | 19        |

## 研究背景

在中国，Android 系统作为智能手机中市场占有率最高的移动操作系统，承载着亿万手机用户的生产生活，大量的 Android 开发人员为其添砖加瓦。但树大招风，Android 智能手机也暴露在各种恶意软件、系统漏洞的威胁之中，无数恶意软件、电信诈骗不断挑战用户的安全意识，但各种隐藏在系统之中的系统漏洞对用户的手机安全影响更为可怕。

由于 Android 操作系统目前仍未有非常完善的补丁机制为其修补系统漏洞，再加上 Android 系统碎片化严重，各手机厂商若要为基于 Android 系统的各种设备修复安全问题则需投入大量人力物力。

随着各种系统漏洞不断被披露，现存的 Android 智能手机就像一艘漏水的船，纵然手机安全软件能够缓解一些安全隐患，但系统中的漏洞仍未被有效修补，攻击大门依旧打开。而 Android 手机中的第三方安全软件又无法被授予系统的最高权限，因而 Android 系统安全问题一直非常棘手。

为了让消费者了解到自己手机的安全性，360 历时两年打造了中国第一个 Android 平台的手机漏洞检测工具“360 透视镜”(<https://shouji.360.cn/vulscanner.htm>)，并向社会公开，任何用户和个人都可下载安装。“360 透视镜”应用依据 Android 官方提供的安全补丁更新通知作为漏洞信息来源，在 Android 系统中实现了无需申请敏感权限即可检测 Android 系统中是否存在漏洞这一核心功能，降低了用户了解自己手机安全状况的限制门槛。

此报告基于“360 透视镜”应用用户主动上传的 62 万份漏洞检测报告，检测内容包括近两年（最新漏洞检测更新至 2019 年 6 月）Android 与 Chrome 安全公告中检出率最高的 104 个漏洞，涵盖了 Android 系统的各个层面，且都与具体设备的硬件无关。我们统计并研究了样本中的漏洞测试结果数据，并对安全状况予以客观具体的量化，希望引起用户和厂商对于手机系统漏洞的关注与重视，为 Android 智能手机用户的安全保驾护航，并希望以此来推进国内 Android 智能手机生态环境的安全、健康地发展。

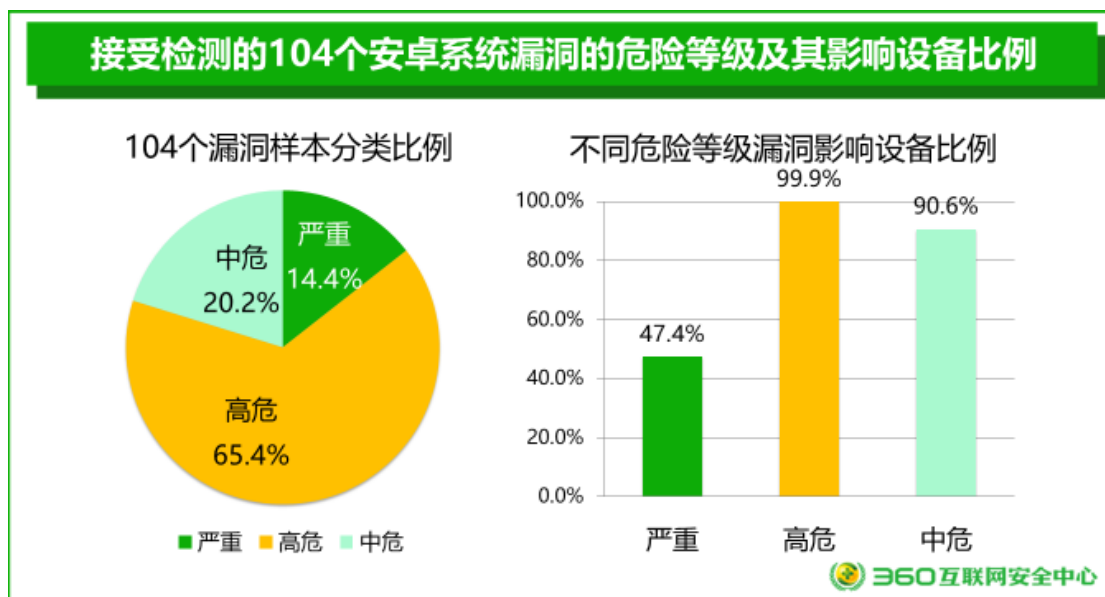
## 第一章 手机系统安全性综述

### 一、系统漏洞的危险等级

此次报告评测的 104 个系统漏洞，按照 Google 官方对系统漏洞的危险评级标准，按照危险等级递减的排序规则，共分为严重、高危、中危三个级别。“严重”级别的漏洞对系统的安全性影响最大，其次为“高危”级别漏洞，然后为“中危”级别漏洞，“低危”级别漏洞未入选。

在这 104 个漏洞中，按照其危险等级分类，有严重级别漏洞 15 个，高危级别漏洞 68 个，中危级别漏洞 21 个。其中高危以上漏洞对用户影响较大，在此次安全评测中对此类漏洞的选取比例达 79.8%。

此次系统安全分析结果显示：90.6% 的 Android 设备受到中危级别漏洞的危害，99.9% 的 Android 设备存在高危漏洞，47.4% 的 Android 设备受到严重级别的漏洞影响。



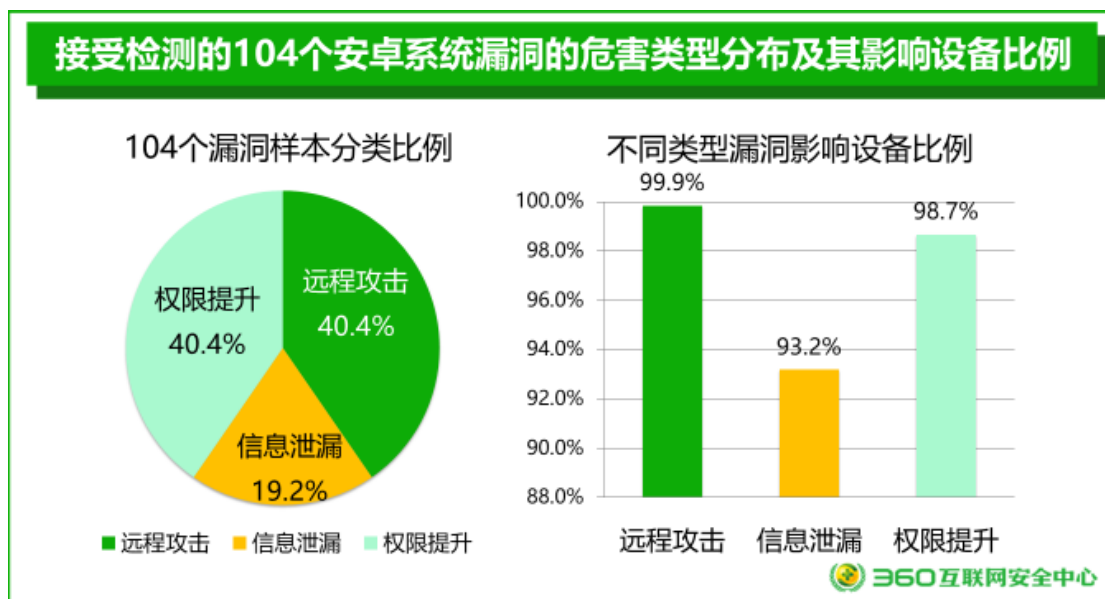
### 二、系统漏洞的危害方式

在本次评测中，本报告参照了 Google 官方对系统漏洞的技术类型分类标准并加以适当合并，将 104 个系统漏洞按照各漏洞的特征分类，共分为远程攻击、权限提升、信息泄漏三个类别。远程攻击漏洞是指攻击者可以通过网络连接对用户的系统进行远程攻击的漏洞，权限提升是指攻击者可以将自身所拥有的权限得以提升的漏洞，信息泄漏则为可以获得系统或用户敏感信息的漏洞。

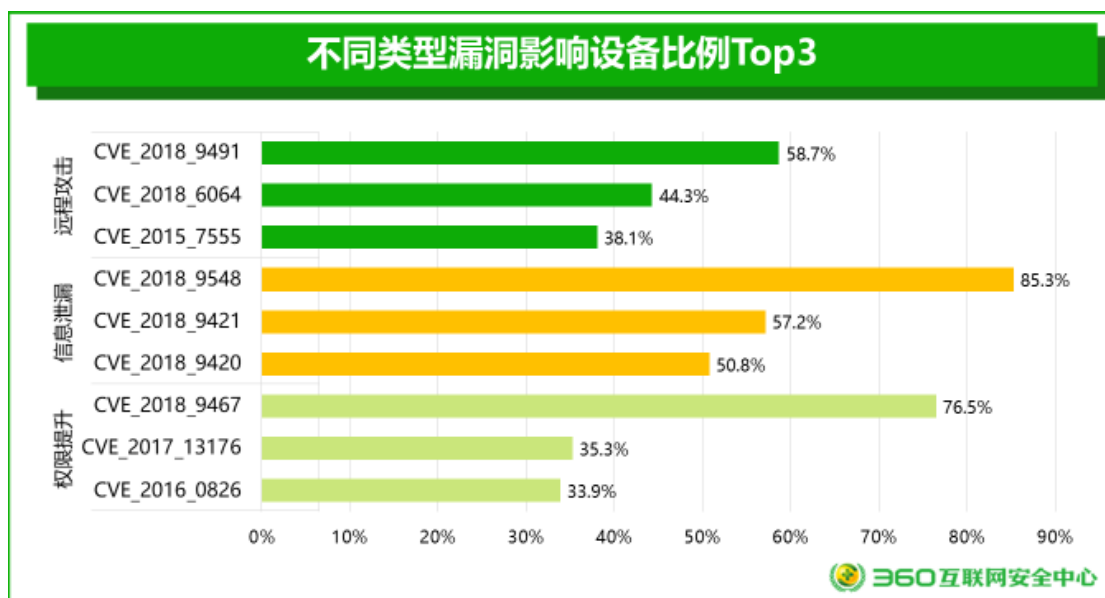
在这 104 个漏洞中，按照其危害方式分类，包括远程攻击漏洞 42 个，权限提升漏洞 42 个，信息泄漏漏洞 20 个。

此次系统安全分析结果显示：99.9% 的设备存在远程攻击漏洞，98.7% 的设备存在权限提升漏洞，93.2% 的设备存在信息泄漏漏洞。与 2018 年检测结果相比，权限提升漏洞占比增加，导致权限提升漏洞影响的设备比例增加比较明显；信息泄漏漏洞影响设备占比有所降

低，远程攻击类漏洞影响设备占比一直居高不下。

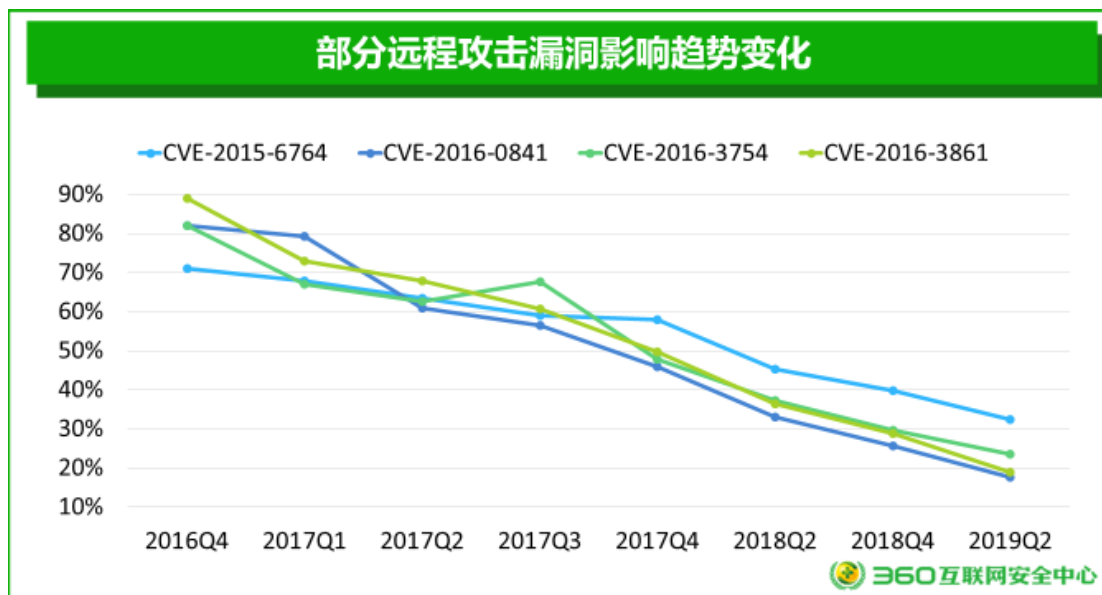


为了观察不同类别的漏洞中哪些影响的设备比例最多，我们分别对三种类别的漏洞进行统计排序，挑选出了各类别中影响设备比例占比前三名的漏洞，其中影响最广泛的漏洞为信息泄漏漏洞 CVE-2018-9548，85.3%的设备都存在这个漏洞，2018 年影响最广的信息泄漏漏洞 CVE-2018-9421 的影响范围由 73.9%跌落到 57.2%；权限提升漏洞中，CVE-2018-9467 的影响范围有所降低，但依然是影响范围最广的权限提升漏洞；CVE-2018-9491 依然为影响范围最广的远程攻击漏洞，影响 58.7%的设备。



三种类型漏洞中，影响设备数量排名第一的只有信息泄漏漏洞 CVE-2018-9548 是新加入的漏洞，这说明历史漏洞的影响范围依然十分庞大。比如 CVE-2015-7555 和 CVE-2016-0826，这两个漏洞分别是 Google 在 2017 年 5 月和 2015 年 12 月安全公告中公开的漏洞，目前依然影响 38.1%和 33.9%的设备。对比 2018 年的数据可以发现，历史漏洞的影响比例整体有所下降，但新旧漏洞如同波浪一般，层出不穷并且形势依然严峻。

远程攻击漏洞是危险等级高、被利用风险最大的漏洞，也是我们最关注的漏洞，为此我们从 2016 年第四季度开始，跟踪了四个比较重要的远程攻击漏洞的影响变化趋势，如下图所示。



整体趋势上看，随着时间的推移，这四个远程攻击漏洞的影响力在不断减小，但是截至 2019 年二季度，这四个漏洞依然影响近 30% 的用户手机安全。但是随着新的远程攻击漏洞的加入，受远程攻击漏洞影响的设备比例会更高，安全形势不容乐观。

### 三、 系统浏览器内核的安全性

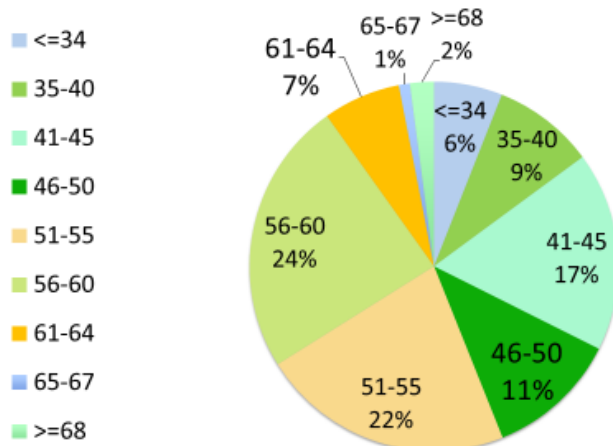
系统浏览器内核是用户每日使用手机时接触最多的系统组件，不仅仅是指用户浏览网页的独立浏览器，实际上，许多安卓应用开发者考虑到开发速度、保障不同设备之间的统一性等因素，会使用系统提供的浏览器内核组件。因而用户在每日的手机使用中，大多会直接或间接地调用系统浏览器内核。

在此次评测中，系统浏览器内核是指 Android 系统的 Webview 组件的核心，在 Android 4.4 之前，Android 系统的 Webview 是基于 Webkit 的，在 Android 4.4 及以后的系统中，Webview 的核心被换成了 Chromium(Chrome 的开源版本，可近似理解为 Chrome)。

在最新统计的样本中，Webkit 所占比重几乎为 0，与 2017 年度相似，说明 4.3 及以下系统手机已经淡出历史舞台。截止至本季度，当前 Google 发布的 Android 平台 Chrome 稳定版的内核的最新版本为 Chrome 76，而在此次检测中有约 0.03% 的用户将自己手机中的浏览器内核升级至最新，这一数据较 2018 年有所下降。而从图中可以看出，Chrome 内核版本大于 55 的设备占 34%，较 2018 年的 25% 提升 9%。总体来说，浏览器内核整体版本有所更新，国内安卓系统生态圈中对浏览器内核的安全程度相对有所增强。



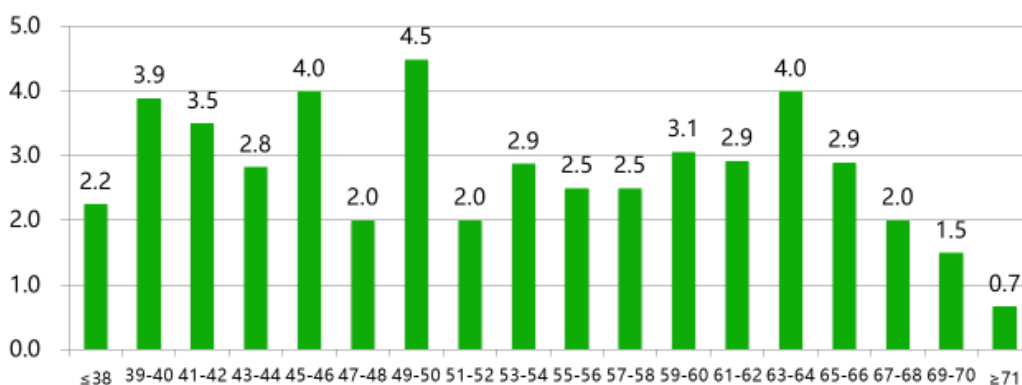
## 安卓系统浏览器内核版本分布



360 互联网安全中心

为了研究不同浏览器内核版本的安全性,我们统计了不同版本的浏览器内核的平均漏洞个数。下图显示了不同 Chrome 版本平均漏洞数量,相对 2018 年的数据,Chrome 57 版本及以下的设备平均漏洞数量几乎没有变化。Chrome 57 版本以上的设备漏洞数量有所增加,这主要是因为本次新加的一些浏览器内核漏洞只影响高版本 Chrome 导致的。同时,2018 年度未检测出漏洞的 Chrome 71 及以上版本在今天也检测出了存在 0.7 个漏洞,浏览器漏洞也是在不断出现并威胁着用户手机的安全。从 Chrome 57 开始,平均漏洞个数逐渐增多,到 Chrome 63 达到一个峰值,之后又逐渐减小,这主要是因为新出现的漏洞让高版本浏览器的漏洞数量有所增加,但整体趋势上还是可以看出,保持最新版本的浏览器内核可以有效增强手机浏览器的安全性。

## 不同版本安卓浏览器平均漏洞个数

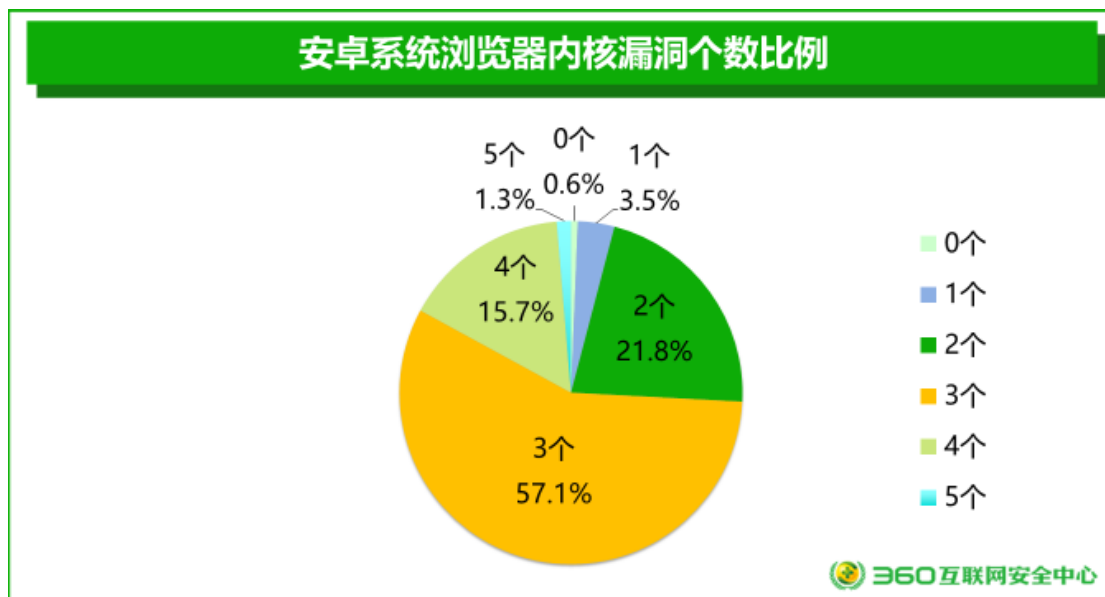


360 互联网安全中心

在本次报告检测的 104 个漏洞当中,有 15 个漏洞是浏览器内核漏洞,这些漏洞大多是可以被远程利用的,危险性极大。安卓系统浏览器内核漏洞的分布情况如下图所示。其中 99.4% 的设备存在至少一个浏览器内核漏洞,15.7% 的设备同时存在 4 个浏览器内核漏洞,漏洞数量最多的设备同时存在 7 个漏洞,但所占比例很小。仅有 0.6% 的设备不受浏览器内

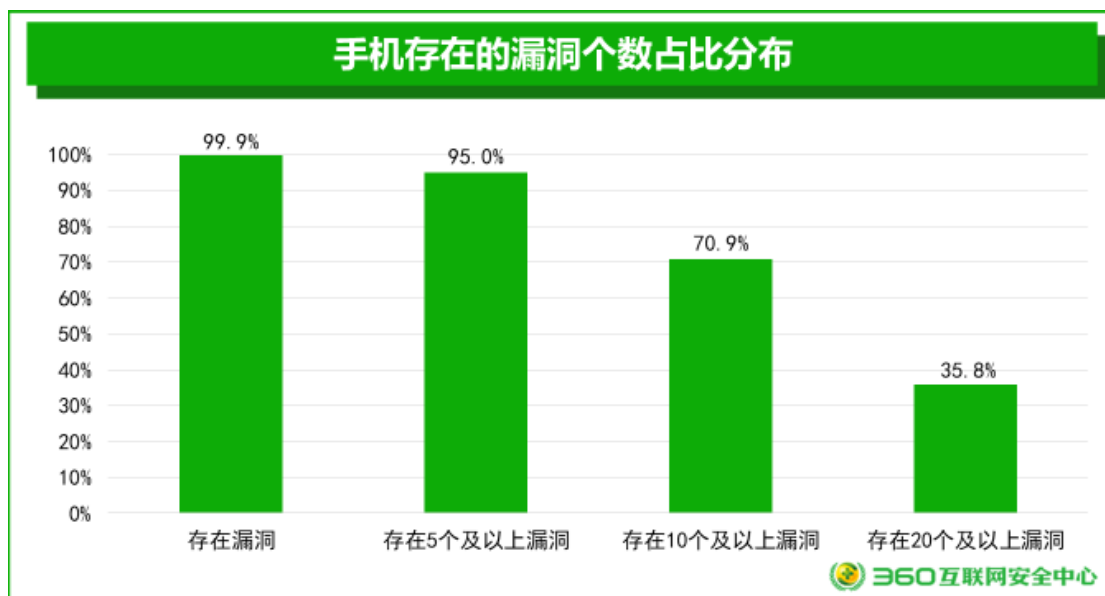


核漏洞影响。与 2018 年数据相比，存在浏览器内核漏洞的设备占比升高 0.3%，同时存在 3 个浏览器内核漏洞设备所占比例大幅提高，这说明新加入的浏览器内核漏洞影响范围广，新漏洞的出现瞬间挑战了大量设备的安全性，用户依然暴露在浏览器漏洞的威胁之中。



#### 四、 系统漏洞的数量分布

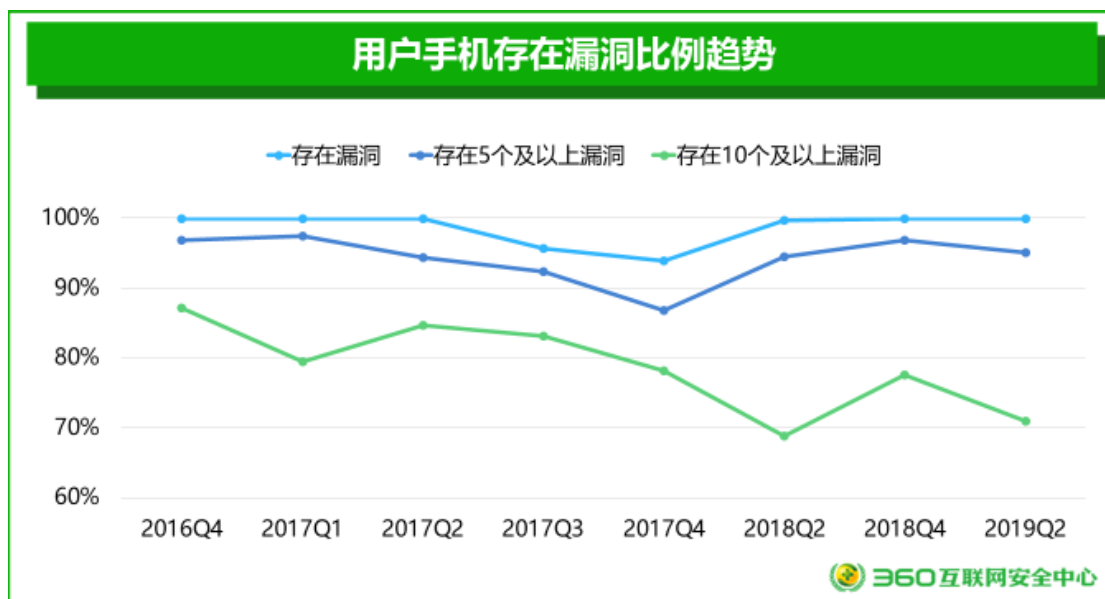
为了研究用户手机中漏洞数量的分布规律，同时对用户手机的安全等级做一个直观的评分，我们统计了所有样本中手机存在漏洞个数的比例分布，结果如下图所示。



在此次测试中，我们检测了 104 个已知漏洞，有 99.97% 的设备存在至少一个安全漏洞，这一数据较 2018 年 99.99% 的比例有所降低，漏洞最多的设备同时包含有 63 个安全漏洞。存在 5 个、10 个、20 个及以上漏洞的比例均有所降低，但依然保持较高的比例。

为了研究近两年用户手机中漏洞数量的变化，同时反映用户手机安全性的变化情况，我

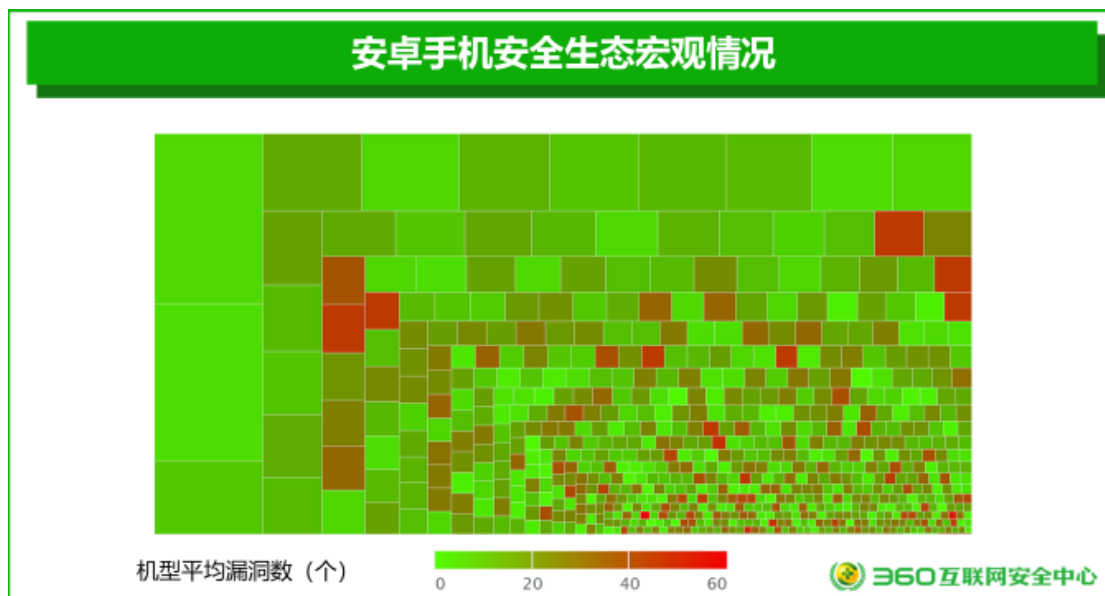
们总结了自 2016 年至今的漏洞数量比例分布及趋势，结果如下图所示。



可以发现，手机存在漏洞的比例整体居高不下，同时若增加检测力度，用户手机整体的安全形势将会表现的更加严峻。如果手机厂商积极做好手机系统的安全补丁更新工作，现行手机系统的安全防护能力就会有明显的提升。虽然国内厂商在不断地对安卓设备进行安全更新，但是安全漏洞也层出不穷，存在漏洞的设备比重仍然居高不下。

## 五、手机安全生态宏观描述

为了研究用户手机中漏洞数量的宏观情况，我们统计了如下宏观描绘图。



其中，各个独立的方块都代表一款具体型号的安卓设备；方块面积表示该型号设备使用人数的多少，使用的人数越多则相应面积越大；其颜色由绿色到红色之间的渐变代表了该型号设备的平均安全水平。由图中可以看出，对于市场占有率高的产品其安全更新情况更加乐

观一些。对比上一季度，新设备的安全补丁更新情况有了很大的进步，厂商对于手机系统安全补丁的重视程度和投入有了明显的改善，多数国内主流厂商均有更新推送新设备的安全补丁，一线厂商则将系统更新至与安卓官方同步（2019-06），但宏观上看安全情况更加严峻，主要原因是新设备所占比例相对较低，正在使用的设备绝大部分还是难以更新的老旧设备。

## 第二章 手机系统版本安全性

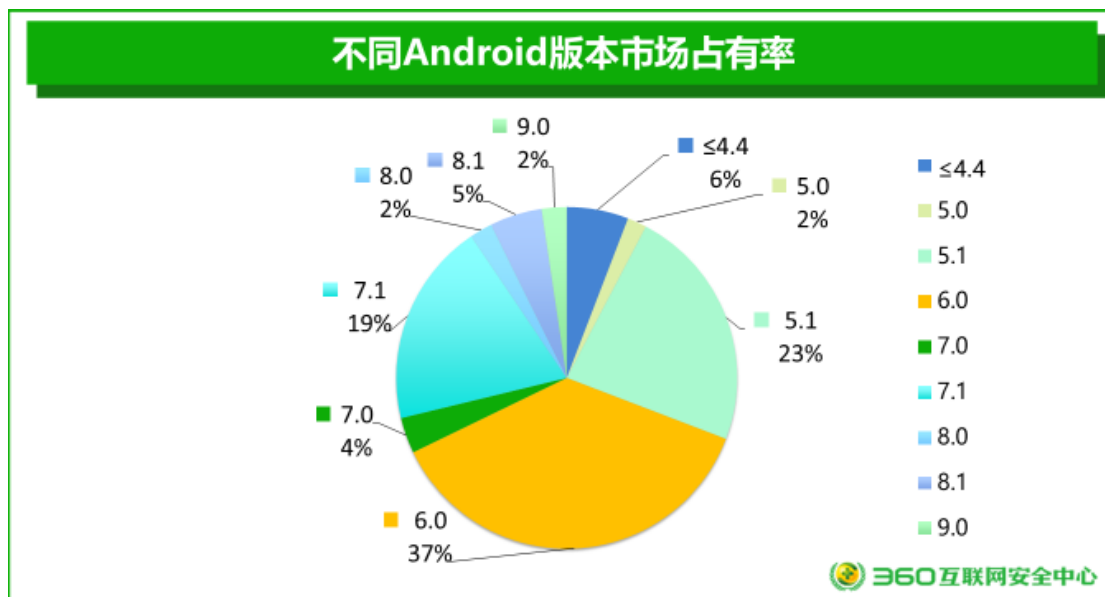
### 一、 各系统版本漏洞情况

由于 Android 系统在升级时不可直接跨版本升级而厂商往往又不愿意为旧机型耗费人力物力适配新系统，因而在一定程度上导致了 Android 系统版本的碎片化。

为了研究不同版本的安卓系统的安全性，我们统计了样本手机所使用的安卓版本分布，并进一步对这些不同的版本的漏洞数量进行了统计分析。

采用 Android 系统版本的分布情况如下图所示，在此次样本中，Android 系统占比最高的 3 个版本分别为 Android 6.0、Android 5.1 和 Android 7.1，比例分别达到 37%、23%和 19%，Android 4.4 及以下版本仅占 6%。Android 8.0 和 Android 8.1 的占比分别达到了 2%和 5%。同时最新版的 Android 9.0 版本比例也占到了 2%。

与 2018 年相同，Android 系统版本占比 Top3 的排名没有发生变化，Android 6.0 依旧为最流行的系统版本，但是 Android 6.0、Android 5.1 所占比例都有所下降，Android 7.1 所占比例有明显提升，这与历史进程以及我们的预期均相符。Android 5.1 和 Android 4.4 所占比例继续降低，但低于 6.0 版本的设备依然占据了约 31%的比例。Android 8.0 和 8.1 的比例有一定幅度的上升，Android 9.0 版本比例也占到了 2%，这不光意味着版本号上的更新，更意味着更多的用户能够享受到新版 Android 系统所带来的一系列安全更新，其中包括更先进的隐私敏感权限动态管理功能和更新功能，而这在一定程度上也极大的增强了用户手机的安全性。在 Android 8.0 引入了一项叫做 Project Treble 的功能，可以缓解安卓系统更新滞后的问题，我们也希望看到这一功能得以最大化发挥作用。但由于 Google 官方对此技术的要求为：出厂预置 8.0 及更高系统的新手机必须支持 Project Treble，出厂预置低于 8.0 的系统在升级 8.0 后可选配置 Project Treble，根据我们观察，目前有许多设备虽然升级到了 8.0，但仍不支持 Project Treble，新系统、新设备仍无法获得 Google 官方的安全更新，故短时间内，安卓系统的碎片化和老旧设备的比例依然会保持较高比例，安全状况依然形势严峻。



通过对每个 Android 版本平均漏洞数量进行统计,得到如下图所示结果。从图中可看出 Android 5.1 及其以下版本平均漏洞数量较多,且整体较上一季度的平均漏洞数保持增加趋势,这很大程度上是由于部分老旧设备无法获得更新而我们检测的漏洞又在持续增加,因此造成了这种现象;而 Android 7.1 及以上系统则更为安全,平均漏洞数量急剧降低。



从图中可以看出,安卓系统版本与漏洞数量并不是简单的线性关系。Android 5.0 以下版本漏洞数量随版本升高而递增,并不是说明 Android 版本越高越不安全,而是因为此次检测主要关注的是最近两年的漏洞,相对版本越老的 Android 系统因为不支持较新的功能而可能不存在相应的漏洞。另外,由于 Google 已经不再为 Android 6.0 及以下系统版本提供安全更新,导致相对于去年的检测数据,Android 6.0 及以下系统的平均漏洞数一直居高不下。反观对于 Android 7.0 及以上系统版本,由于持续的安全补丁推送,平均漏洞数相对低很多。

实际上系统的安全性受到厂商重视度、系统功能的多少与变动,甚至服役时间、普及程度、恶意攻击者的攻击价值等等因素的共同影响,但修补了历史已知漏洞的最新系统往往会相对安全些。

## 二、 安卓系统漏洞缓解措施

随着 Android 版本号的提升,其安全手段与漏洞缓解措施也在逐渐增加。通常来说,版本越新的安卓系统,其安全防护手段越强,系统漏洞利用的难度也越大。

例如,从 Android 4.3 开始,安卓开始引入 SELinux 沙盒机制,并在后续的版本中不断对其进行加固,从 Android 5.0 开始,引入全盘加密,以保证用户的信息安全。Android 7.0 中提供了基于文件的加密,进一步保证了用户的信息安全;并实现了深层次的地址随机化机制,使得本地权限提升的攻击难度显著提高。该版本 Android 系统中 Google 工程师对 Media Server 进行了重构,将其按照最小权限原则将之分隔成多个独立的进程与组件,从而即使其中某一个进程或组件存在漏洞,攻击者也无法直接在别的进程空间内执行代码;并且在整个 MediaServer 的编译过程中新增了整型溢出防护机制,从而从编译阶段杜绝类似于 Stagefright 漏洞利用情况的出现。在 Android 8.1 中,系统的安全性又进一步增强,如引进 Project Treble,进一步提升了对设备特定组件的攻击保护;Webview 方面也有提升,Android 8.0 中 Webview 运行在独立的沙箱进程中,对系统其余部分的访问非常有限。最新的 Android 9.0 也加入了

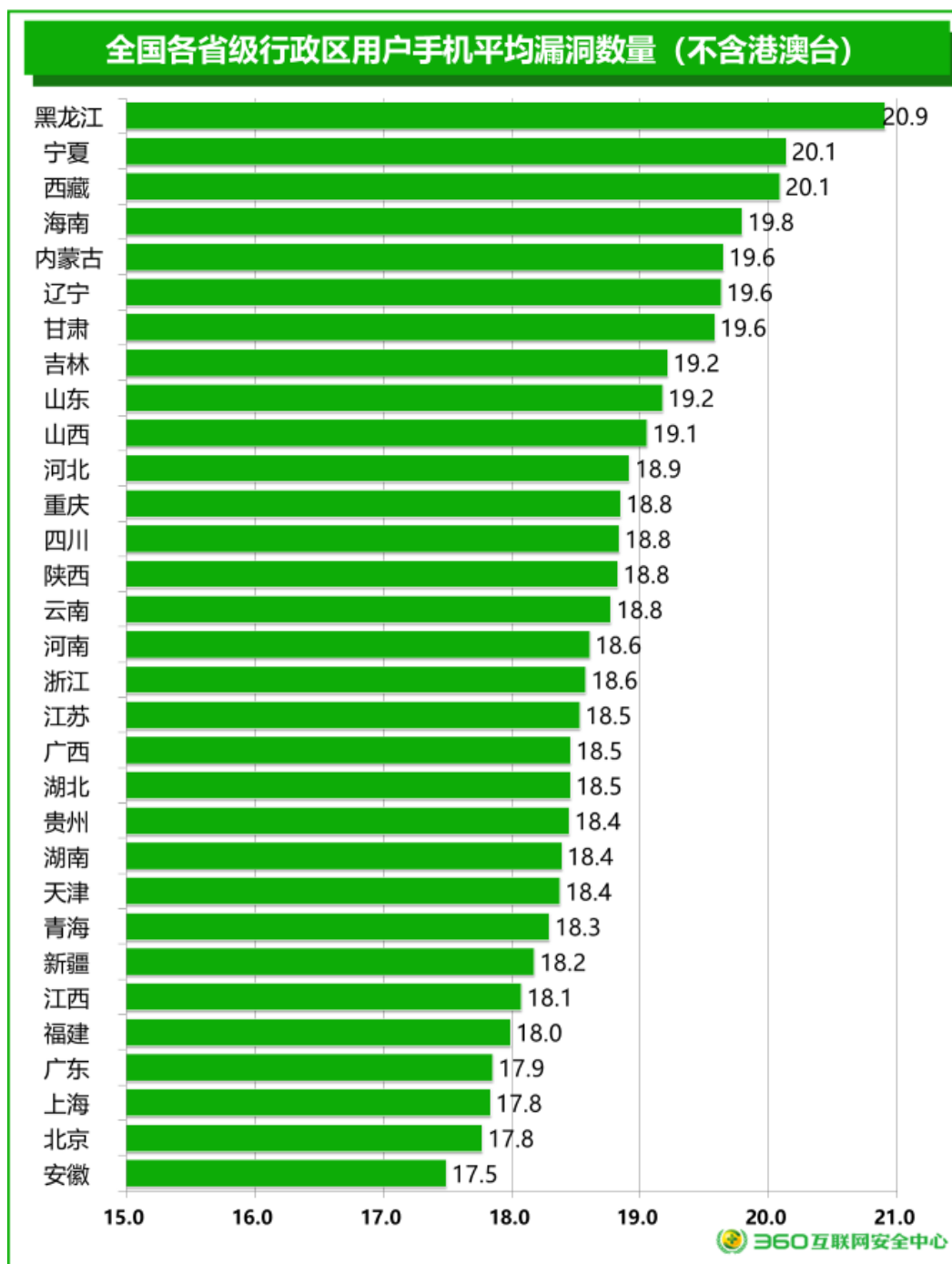
很多安全特性，如新的硬件安全性模块，控制流完整性校验，具有密钥轮转的 APK 签名方案等，可以更加有效的保护用户的设备及应用安全。

不论从漏洞数目，还是漏洞防护机制上，最新版本的安卓系统均比低版本安卓系统安全性更好。而国内由于安卓碎片化的情况，仍存在大量低版本的带有漏洞的安卓设备。

### 第三章 手机系统安全性地域分布

正如电信诈骗、伪基站等有明显的地域分布特征，为了更加细致地探究系统漏洞与不同省市之间的关系，我们根据样本数据中地域信息进行了统计和分析。

下图为各省份平均每台手机漏洞数量，数值越大，说明该地域安卓手机的安全性相对越低、越不安全；数字越小，则代表该地域安卓手机的安全性越高。手机安全性最低的前三名为黑龙江、宁夏、西藏，平均每台手机拥有漏洞数分别为 20.9、20.1、20.1 个。而安全性最高的前三名为安徽、北京、上海，平均每台手机拥有漏洞数分别为 17.5、17.8、17.8 个。大致上，经济越发达的地区，用户所使用的手机的平均漏洞数量越少，手机安全性相对越高。





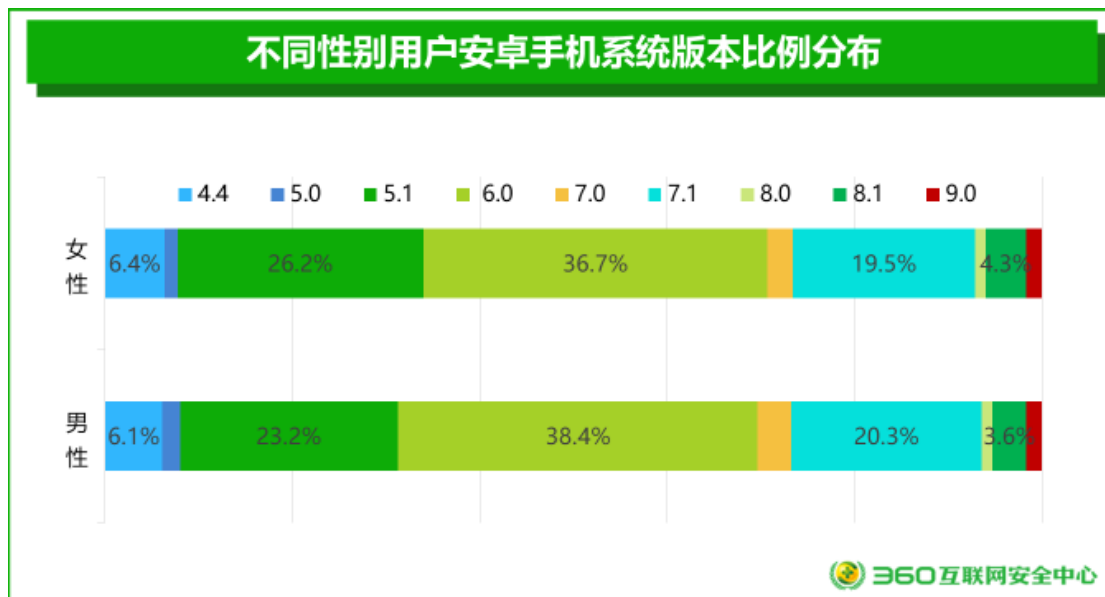


用热力图表示如上图所示，可以更好的看出平均漏洞数的地域分布特征。颜色越红的地区，手机的安全性越低，颜色越浅的地区，手机安全性越高。

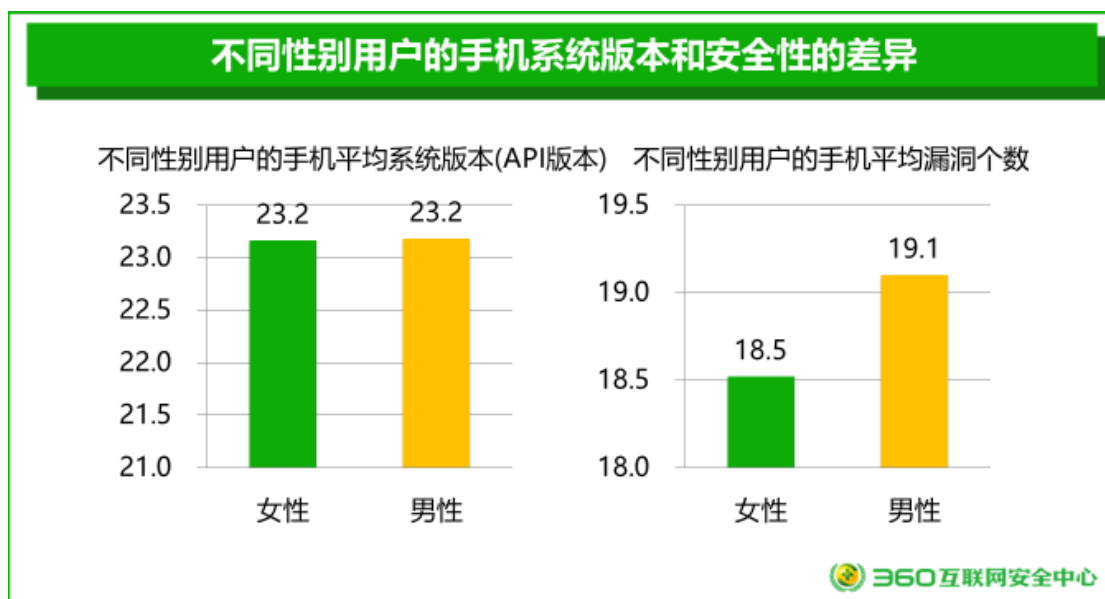
## 第四章 手机系统安全性与用户性别的相关性

由于性别上天生的性格、喜好等的差异，不同性别用户在选择手机时可能会有不同的侧重点，比如女性用户可能在外观、轻薄、颜色等方面着重考虑，而男性可能更侧重性能、屏幕尺寸等因素。一部手机在其服役周期内也可能会因时间的推移而被不同的使用者所使用，而厂商在手机的升级维护中，不同手机又会有不同的策略。

为了探究手机系统的安全性用户性别之间有无联系，我们调研了 1000 位用户的性别信息，统计了不同性别用户与其手机的安全性之间可能的关系。



从上图中，我们可以清晰的看出：在此次评测中，男性与女性使用的手机系统版本分布差异不大，与 2018 年数据相比，整体比例无过大变化，只是 7.1 及以上的新版本系统所占比例提升比较明显。



不同性别用户手机系统中存在的漏洞情况如上图所示。我们可以看到男性与女性手机的平均系统版本数值均约为 23.2 (数值为系统 API 版本, 为 Google 官方为便于安卓版本的计数而提供的一个版本的数字代号, 其中 5.0 为 21, 5.1 为 22, 6.0 为 23, 7.0 为 24), 即平均使用的系统版本在 Android 6.0 和 7.0 之间。

对比 2018 年数据, 男性和女性的平均系统版本均有所提升, 但平均来看, 女性用户手机系统版本提升幅度为 0.7, 而男性用户手机系统版本提升幅度较小, 仅提升了 0.5。

在此次统计中, 无论男性还是女性用户, 平均漏洞个数均有所降低。其中, 女性手机平均漏洞个数降低较为明显, 较 2018 降低幅度为 16%, 而男性用户平均漏洞数量降低幅度仅为 9%。从此次统计数据可以看出, 2019 年女性用户手机系统版本增长明显, 漏洞数量降低明显, 说明女性用户的手机更新换代更为频繁, 新上市的手机因为系统版本更新, 厂商支持力度更大, 所以存在漏洞数量也就越低。

## 第五章 手机系统安全漏洞的修复

受到 Android 系统的诸多特性的影响，系统版本的碎片化问题日益突出。就每一款手机而言，厂商在其维护周期内，通常会隔一段时间向用户推送一次升级版本，而用户在大多数情况下可以自主选择升级或不升级。综合这些特性，在 Android 系统的安全漏洞方面，也产生了严重的碎片化问题。

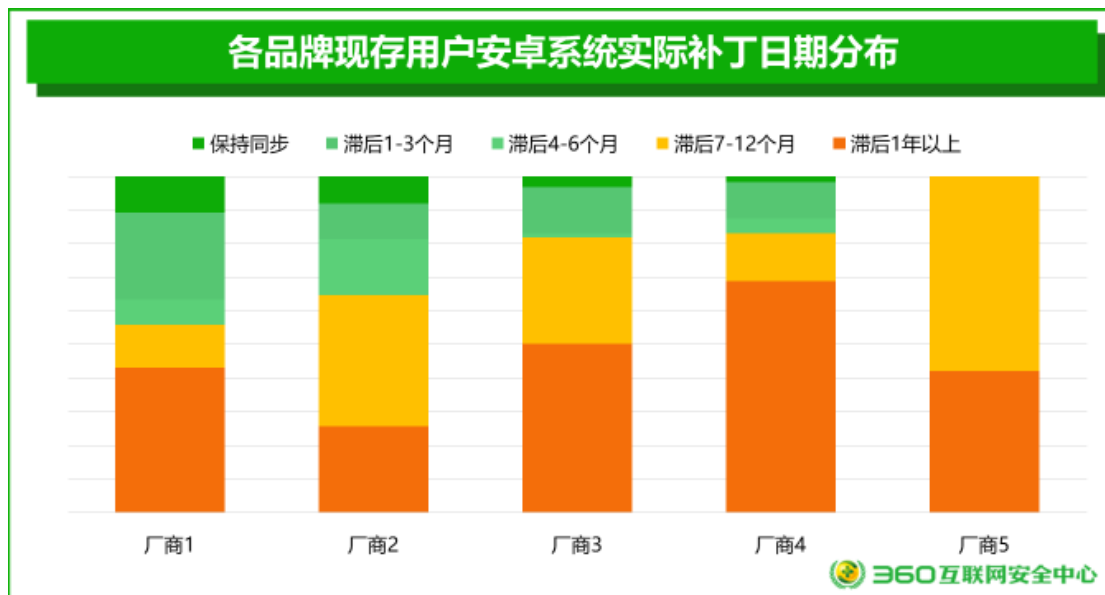
在 Android 系统中，存在一个名为“Android 安全补丁级别”的字段，它是 Google 公司向第三方安卓手机厂商推送的一个 Android 安全补丁的日期号，旨在为安卓设备的已知漏洞的修复情况做一个简单的说明。当前 Google 对于 Android 7.0 及其上版本号的安卓系统会定期推送更新，如果厂商遵循 Google 公司的建议正确打入补丁，那么手机中显示的安全补丁级别越高，即日期越新，手机的安全情况就相对越安全。

为了探究手机系统中已知安全漏洞的修复情况，我们对样本中不同设备型号、不同系统安全漏洞的修复情况做了相关研究。

### 一、 厂商漏洞修复情况

为了探究国内厂商为现存设备修复安全漏洞的情况，我们统计了样本中不同厂商手机目前的安全补丁级别情况。

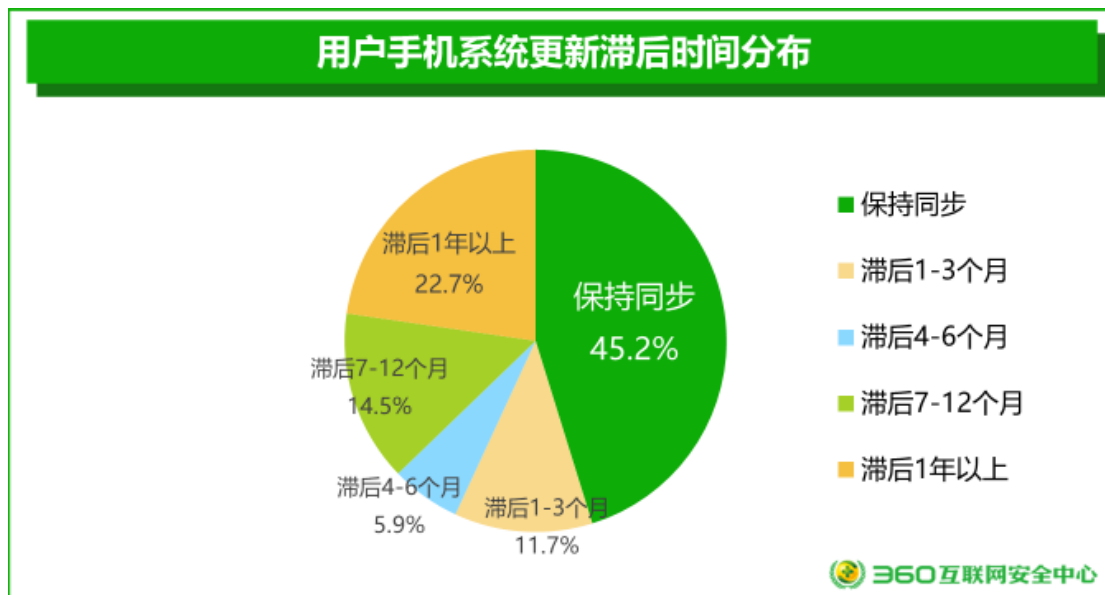
下图为各厂商手机中实际存在的安全补丁级别情况，该情况是将各厂商现存手机中实际补丁日期与 Google 官方最新版本（2019 年 6 月）版本对比，综合安全补丁级别最高、最新的手机品牌前 5 名。图中绿色方块面积越大，说明该厂商的手机补丁级别相对越高，漏洞修复相对越及时；相反，如果黄色和橙色面积越大，则说明补丁级别越低，漏洞修复越滞后。



从图中我们可以看出，在及时推送安全补丁级别方面，TOP5 的厂商在本年度检测结果呈现比较明显的两极分化，比如厂商 1 的整体看安全补丁更新比较及时，且有很大比例安全更新与谷歌保持同步。厂商 5 的安全补丁更新情况比较差，大部分都是滞后官方 7 个月以上，没有与官方补丁更新保持同步的设备，可以看出其对手机安全的重视程度比较差。

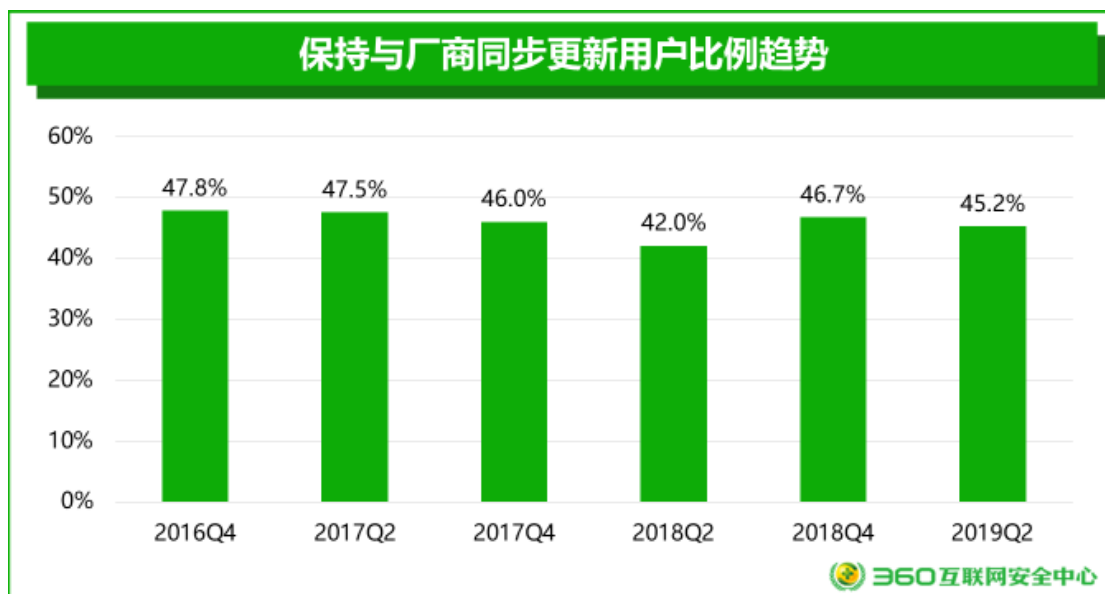
## 二、 用户主动升级意愿

为了探究用户主动升级系统的意愿，我们统计了不同厂商、不同机型、不同安全补丁级别的分布情况。此统计为在每个机型中，观察用户是否主动保持这个厂商对此机型提供最新版本。



整体上，可以明显发现近半的用户还是很有安全意识的，从统计数据中可以看出，约有 45.2% 的用户能够保持手机系统中安全补丁等级的版本与厂商所能提供的最新版本保持一致，这一比例相较 2018 年降低了 1.5 %。仍有 11.7% 的用户的系统版本滞后厂商最新版本 1-3 个月，大约 5.9% 的用户手机版本滞后 4-6 个月，约 14.5% 的用户手机版本滞后半年以上，有 22.8% 的用户手机版本滞后官方最新版本达一年以上。总体而言，更新滞后的平均时间在变长，而这些用户将比保持系统更新的用户暴露在更多的漏洞与更高的攻击风险之中。

我们还统计了近两年来用户手机系统与厂商保持同步更新的比例变化情况，如下图所示。



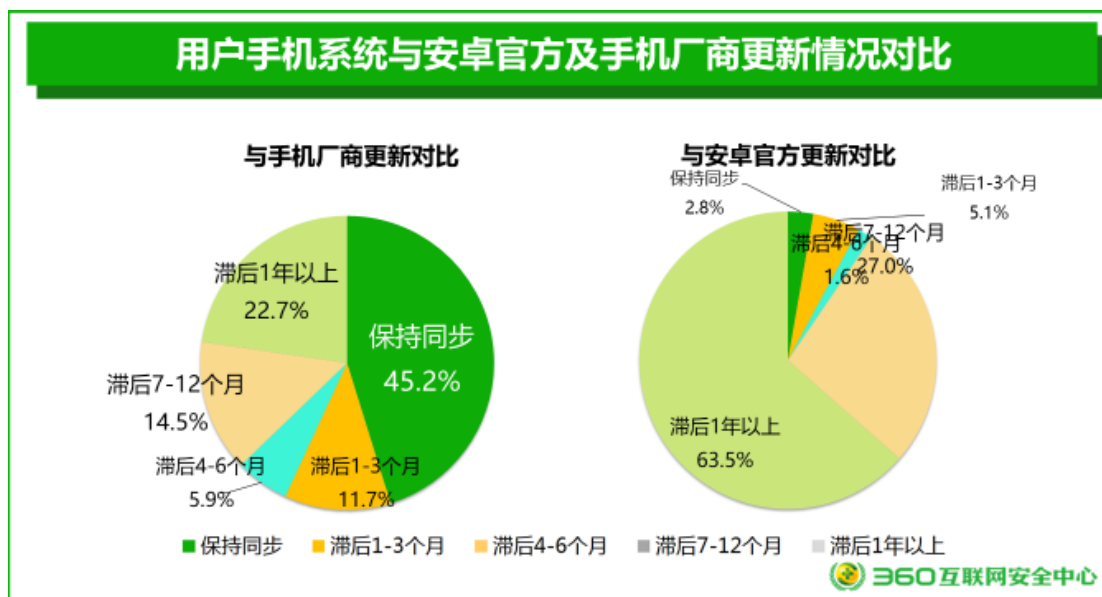
整体来说，近半用户还是会愿意保持系统更新至最新版本，但是保持更新的比例有小幅下降，更新比例仍然偏低，一半以上的用户手机处于高风险状态。

对于安卓手机用户来说，其手机操作系统大多由手机厂商在其维护周期内提供更新。但往往会有用户手机服役周期超出厂商维护周期（通常为两年）的情况，此时，考虑到手机硬件条件、用户体验等问题，大多数厂商通常都不会再提供系统更新服务，也因此会导致某些手机机型系统无法与最新的安卓版本保持一致。

从用户角度来看，我们建议手机厂商在不影响用户体验的基础上，尽量为用户提供系统漏洞安全补丁方面的更新，以保护用户手机安全不受影响。

### 三、 漏洞修复综合分析

虽然很多手机厂商会给用户推送安全更新，但是大部分厂商很难保证安全补丁的更新时间能与安卓官方保持同步，这也导致很多用户实际上并不能及时得到已公开漏洞的安全补丁。下图给出了用户手机系统与安卓官方系统、手机厂商系统的更新情况对比。



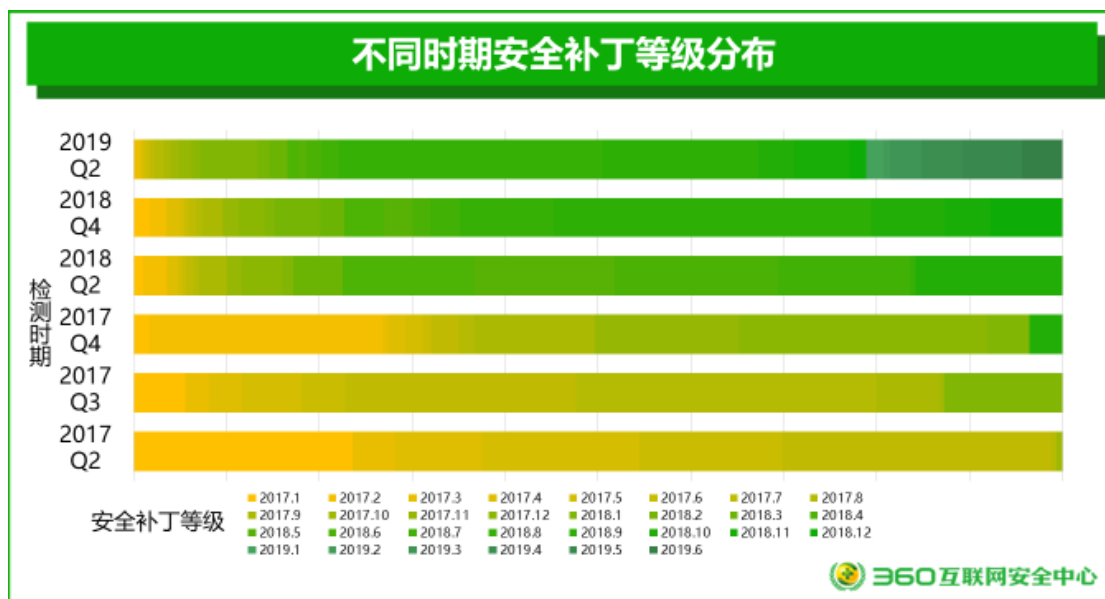
可以看到，近一半的手机用户能够保持手机系统与厂商最新系统的同步更新，且近 6 成用户能够在厂商推出更新版本后三个月内更新自己的手机。但能够享受与安卓官方最新系统保持同步更新服务的用户则仅为 2.8%，但这一数据较 2018 年上升 1.8%；滞后时间小于 3 个月的用户占比 7.9%，上升 0.4%；同时注意到滞后 1 年以上的手机系统比例明显有所提升，这也是由于老旧机型逐步淘汰的结果。可以看出，Google 公司推出安全更新的速度正在加快，但厂商和手机用户安全更新的速度相对较慢。

综合对比用户手机系统的更新状态、安卓官方的更新状态和手机厂商的更新状态，我们发现：与安卓官方最新更新时间相比，用户的手机系统平均滞后了约 18.2 个月，但与手机厂商已经提供该机型的最新版本相比，则平均只滞后了 6.0 个月，这两个数据较 2018 年第四季度有所上升，但用户手机因未能及时更新而存在安全漏洞的重要原因仍然是手机厂商普遍未能实现其定制开发的安卓系统与安卓官方同步更新，而且延时较大。

## 第六章 新品手机安全更新情况

由于安卓官方在早期安卓版本中对于安全补丁没有统一的补丁策略，导致大部分早期手机厂商发布手机产品后即使想对手机系统安全情况予以修补也会受到较大的阻力。当今主流消费者所购买的手机一般是最新发布的型号，为了探究主流厂商在今天对于新机型的安全更新情况，我们特意选取了自 2017 年以来的数据并分析安卓 7.0 及以上手机的安全补丁更新情况。

为了探究主流机型的安全更新情况，我们以不同时间下安全补丁等级的分布情况作为数据信息，经汇总分析后，结果如下图所示。



图中横坐标代表检测结果中出现的不同安全补丁等级，纵坐标代表我们不同的检测时期（从 2017 年第二季度至今）。即图中色块表示在检测结果中的安全补丁等级的分布情况，综合多次检测结果即可判断系统安全补丁等级的变化趋势。

从图中我们可以看出，主流机型在 2017 年第二季度至 2019 年第二季度的过程中，图中呈现比较明显的以浅色为主变为深色占比明显的迁变趋势。即设备中安全补丁等级是在随着时间的推进而不断更新的，没有出现大范围停止更新的情况。事实上，一方面安卓系统安全补丁等级机制为厂商更新系统提供了便利，另一方面厂商对于主流机型安全更新的也确实在持续投入，因此新品手机的持续安全更新情况，较以往有了较大的改善。这说明主流手机厂商不再是消费者所抱怨“只管卖不管维护”的极端情况了，厂商在手机安全方面做了一定的努力，有了显著的效果。对于消费者来说，在进行手机的更新换代时可以更加放心的去选择有持续安全更新的厂商。



## 附录

此次分析中所检测的 104 个漏洞的编号如下表所示。

| 漏洞编号           | 公布时间       | 级别 | 漏洞类型 | 漏洞简述                         |
|----------------|------------|----|------|------------------------------|
| CVE-2016-0838  | 2016/01/12 | 严重 | 远程攻击 | Sonivox 组件中的远程攻击漏洞           |
| CVE-2016-0841  | 2016/02/26 | 严重 | 远程攻击 | MetadataRetriever 组件中的远程攻击漏洞 |
| CVE-2015-1805  | 2016/03/18 | 严重 | 权限提升 | Pipe 条件竞争 Root 漏洞            |
| CVE-2016-2430  | 2016/03/25 | 严重 | 权限提升 | Debuggerd 中的权限提升漏洞           |
| CVE-2016-2463  | 2016/06/01 | 严重 | 远程攻击 | 媒体服务进程中的远程攻击漏洞               |
| CVE-2016-3861  | 2016/09/01 | 严重 | 远程攻击 | 国际编码漏洞                       |
| CVE-2016-5195  | 2016/12/05 | 严重 | 权限提升 | 脏牛漏洞                         |
| CVE-2017-0471  | 2017/03/01 | 严重 | 远程攻击 | 媒体服务中的远程攻击漏洞                 |
| CVE-2017-0589  | 2017/05/01 | 严重 | 远程攻击 | 媒体服务中的远程攻击漏洞                 |
| CVE-2015-7555  | 2017/05/05 | 严重 | 远程攻击 | GIFLIB 远程攻击漏洞                |
| CVE-2017-0832  | 2017/11/01 | 严重 | 远程攻击 | 多媒体服务框架中的权限提升漏洞              |
| CVE-2017-13176 | 2018/01/01 | 高危 | 权限提升 | Android 运行时漏洞                |
| CVE-2015-1532  | 2015/01/27 | 高危 | 远程攻击 | 9Patch 图片漏洞                  |
| CVE-2015-3849  | 2015/08/13 | 高危 | 权限提升 | 安卓系统 Region 漏洞               |
| CVE-2015-6764  | 2015/11/18 | 高危 | 远程攻击 | Chrome v8 破坏者漏洞              |
| CVE-2015-6771  | 2015/12/01 | 高危 | 远程攻击 | Chrome V8 引擎的远程攻击漏洞          |
| CVE-2016-2412  | 2016/02/26 | 高危 | 权限提升 | 安卓系统服务杀手漏洞                   |
| CVE-2016-2416  | 2016/02/26 | 高危 | 信息泄漏 | 未授权信息泄漏                      |
| CVE-2016-0826  | 2016/03/01 | 高危 | 权限提升 | 媒体服务进程中的权限提升漏洞               |
| CVE-2016-0830  | 2016/03/01 | 高危 | 远程攻击 | 蓝牙组件中的远程攻击漏洞                 |
| CVE-2016-2449  | 2016/03/25 | 高危 | 权限提升 | 照相机应用中的栈溢出漏洞                 |
| CVE-2016-0847  | 2016/04/02 | 高危 | 权限提升 | 电话应用中的权限提升漏洞                 |
| CVE-2016-1646  | 2016/04/15 | 高危 | 远程攻击 | Chrome V8 引擎中内存越界操作漏洞        |
| CVE-2016-2439  | 2016/05/01 | 高危 | 远程攻击 | 蓝牙组件中的远程攻击漏洞                 |
| CVE-2016-2476  | 2016/06/01 | 高危 | 权限提升 | 媒体服务进程中的权限提升漏洞               |
| CVE-2016-2495  | 2016/06/01 | 高危 | 远程攻击 | 媒体服务进程中的远程攻击漏洞               |
| CVE-2016-3744  | 2016/07/01 | 高危 | 远程攻击 | 蓝牙组件中的远程攻击漏洞                 |
| CVE-2016-3754  | 2016/07/01 | 高危 | 远程攻击 | 媒体服务进程中的远程拒绝服务漏洞             |
| CVE-2016-3915  | 2016/10/03 | 高危 | 权限提升 | 照相机应用中的权限提升漏洞                |
| CVE-2016-6754  | 2016/11/01 | 高危 | 远程攻击 | BadKernel 漏洞                 |
| CVE-2016-6710  | 2016/11/03 | 高危 | 信息泄漏 | 下载管理器中的信息泄漏漏洞                |
| CVE-2016-9651  | 2016/12/01 | 高危 | 远程攻击 | PwnFest2016 Chrome v8 漏洞     |
| CVE-2017-0386  | 2017/01/03 | 高危 | 权限提升 | libnl 库中的权限提升漏洞              |
| CVE-2017-0387  | 2017/01/03 | 高危 | 权限提升 | Android Mediaserver 权限提升漏洞   |
| CVE-2017-0421  | 2017/02/01 | 高危 | 信息泄漏 | 安卓框架中的信息泄漏漏洞                 |
| CVE-2017-0412  | 2017/02/01 | 高危 | 权限提升 | Android Framework APIs 权限许可和 |

|                |            |    |      |                                 |
|----------------|------------|----|------|---------------------------------|
|                |            |    |      | 访问控制漏洞                          |
| CVE-2017-5030  | 2017/03/09 | 高危 | 远程攻击 | Chrome V8 引擎中内存破坏漏洞             |
| CVE-2017-5053  | 2017/03/29 | 高危 | 远程攻击 | pwn2own2017 远程执行漏洞              |
| CVE-2016-4658  | 2017/06/01 | 高危 | 远程攻击 | libxml2 中的远程攻击漏洞                |
| CVE-2017-0666  | 2017/07/01 | 高危 | 权限提升 | Android Framework 权限许可和访问控制漏洞   |
| CVE-2017-0669  | 2017/07/01 | 高危 | 信息泄漏 | Android Framework 信息泄漏漏洞        |
| CVE-2017-0725  | 2017/08/01 | 高危 | 远程攻击 | BMP 图片拒绝服务漏洞                    |
| CVE-2017-0771  | 2017/09/01 | 高危 | 远程攻击 | ICO 图片中的拒绝服务漏洞                  |
| CVE-2017-5116  | 2017/09/05 | 高危 | 远程攻击 | Chrome V8 引擎中类型混淆漏洞             |
| CVE-2017-0774  | 2017/10/01 | 高危 | 远程攻击 | MPEG4 中的拒绝服务漏洞                  |
| CVE-2017-0672  | 2017/10/01 | 高危 | 远程攻击 | BMP 图片中的拒绝服务漏洞                  |
| CVE-2017-13156 | 2017/12/01 | 高危 | 权限提升 | Android System(art) 权限许可和访问控制漏洞 |
| CVE-2017-0870  | 2017/12/01 | 高危 | 权限提升 | 安卓服务框架(libminikin)中的权限提升漏洞      |
| CVE-2017-13199 | 2018/01/01 | 高危 | 远程攻击 | BMP 图片解析漏洞.                     |
| CVE-2018-6064  | 2018/01/10 | 高危 | 远程攻击 | Chrome V8 引擎中类型混淆漏洞             |
| CVE-2017-13232 | 2018/02/01 | 高危 | 信息泄漏 | 系统音频服务中的信息泄漏漏洞                  |
| CVE-2017-13249 | 2018/03/01 | 高危 | 远程攻击 | MPEG 视频文件解析漏洞.                  |
| CVE-2017-13274 | 2018/04/08 | 高危 | 权限提升 | Android 权限许可和访问控制漏洞             |
| CVE-2017-13287 | 2018/04/08 | 高危 | 权限提升 | Android 权限许可和访问控制漏洞             |
| CVE-2017-13311 | 2018/05/01 | 高危 | 权限提升 | Android 权限许可和访问控制漏洞             |
| CVE-2017-13315 | 2018/05/01 | 高危 | 权限提升 | Android 权限许可和访问控制漏洞             |
| CVE-2018-9338  | 2018/06/01 | 高危 | 权限提升 | 蓝牙组件中的权限提升漏洞                    |
| CVE-2018-9349  | 2018/06/01 | 高危 | 信息泄漏 | libvpx 中的信息泄漏漏洞                 |
| CVE-2016-2426  | 2016/04/02 | 中危 | 信息泄漏 | 安卓框架中的信息泄漏漏洞                    |
| CVE-2016-1677  | 2016/05/25 | 中危 | 信息泄漏 | Chrome V8 decodeURI 信息泄漏漏洞      |
| CVE-2016-1688  | 2016/05/25 | 中危 | 远程攻击 | Chrome V8 引擎的信息泄漏漏洞             |
| CVE-2016-2496  | 2016/06/01 | 中危 | 权限提升 | 安卓框架界面中的权限提升漏洞                  |
| CVE-2016-3760  | 2016/07/01 | 中危 | 权限提升 | 蓝牙组件中的权限提升漏洞                    |
| CVE-2016-3832  | 2016/08/01 | 中危 | 权限提升 | 安卓框架界面中的权限提升漏洞                  |
| CVE-2016-2497  | 2016/08/05 | 中危 | 权限提升 | 安卓框架界面中的权限提升漏洞                  |
| CVE-2016-3897  | 2016/09/01 | 中危 | 信息泄漏 | WIFI 模块中的信息泄漏漏洞                 |
| CVE-2016-3921  | 2016/10/03 | 中危 | 权限提升 | 安卓框架界面中的权限提升漏洞                  |
| CVE-2017-0423  | 2017/02/01 | 中危 | 权限提升 | 蓝牙中的权限提升漏洞                      |
| CVE-2017-0495  | 2017/03/01 | 中危 | 信息泄漏 | 媒体服务中的信息泄漏                      |
| CVE-2017-0490  | 2017/03/01 | 中危 | 权限提升 | Android Wi-Fi 权限许可和访问控制漏洞       |
| CVE-2017-0560  | 2017/04/01 | 中危 | 信息泄漏 | 恢复出厂设置进程中的信息泄漏漏洞                |
| CVE-2017-0553  | 2017/04/01 | 中危 | 权限提升 | libnl 中的提权漏洞                    |
| CVE-2017-5056  | 2017/06/01 | 中危 | 远程攻击 | Google xml 中的 UAF 漏洞            |

|                |            |    |      |                                     |
|----------------|------------|----|------|-------------------------------------|
| CVE-2017-0739  | 2017/08/01 | 中危 | 信息泄漏 | Libhevc 中的信息泄漏漏洞                    |
| CVE-2017-0820  | 2017/10/01 | 中危 | 远程攻击 | 多媒体服务框架中的远程攻击漏洞                     |
| CVE-2017-13241 | 2018/02/01 | 中危 | 信息泄漏 | AVC 和 MPEG4 编码器中的漏洞                 |
| CVE-2017-13268 | 2018/03/01 | 中危 | 信息泄漏 | System(bluetooth)存在信息泄漏漏洞           |
| CVE-2018-6136  | 2018/04/12 | 中危 | 远程攻击 | Chrome V8 引擎中越界访问漏洞                 |
| CVE-2018-9458  | 2018/08/01 | 高危 | 权限提升 | Android Framework 权限许可和访问控制漏洞       |
| CVE-2018-9420  | 2018/07/01 | 高危 | 信息泄漏 | Android Framework 信息泄漏漏洞            |
| CVE-2018-9421  | 2018/07/01 | 高危 | 信息泄漏 | Android Media framework 信息泄漏漏洞      |
| CVE-2018-9427  | 2018/08/01 | 严重 | 远程攻击 | CopyToOMX 中越界写引入的远程代码执行             |
| CVE-2018-17463 | 2018/09/25 | 高危 | 远程攻击 | Hack2Win 2018 v8 远程执行漏洞             |
| CVE-2018-9467  | 2018/09/01 | 高危 | 权限提升 | URL Hostname 解析漏洞                   |
| CVE-2018-9471  | 2018/09/01 | 高危 | 权限提升 | NanoAppFilter Parcel 读取数据时数据类型不一致漏洞 |
| CVE-2018-9491  | 2018/10/01 | 高危 | 远程攻击 | Android 远程代码执行漏洞                    |
| CVE-2018-9499  | 2018/10/01 | 高危 | 信息泄漏 | MediaDrmServer 信息泄漏漏洞               |
| CVE-2018-9522  | 2018/11/01 | 高危 | 权限提升 | 调用未实现函数                             |
| CVE-2018-9547  | 2018/12/01 | 高危 | 权限提升 | Android System server 权限提升漏洞        |
| CVE-2018-9548  | 2018/12/01 | 高危 | 信息泄漏 | ContentProvider 中 URI 绕过漏洞          |
| CVE-2018-9584  | 2019/01/01 | 高危 | 权限提升 | NFC 组件权限提升漏洞                        |
| CVE-2018-9585  | 2019/01/01 | 高危 | 信息泄漏 | NFC 组件信息泄漏漏洞                        |
| CVE-2019-5782  | 2019/01/09 | 高危 | 远程攻击 | 天府杯 2018 错误假设漏洞                     |
| CRBUG-944971   | 2019/01/09 | 高危 | 远程攻击 | Pow2Own 2018 特斯拉漏洞                  |
| CVE-2019-1993  | 2019/02/01 | 高危 | 权限提升 | 蓝牙权限许可和访问控制问题漏洞                     |
| CVE-2019-2016  | 2019/03/01 | 高危 | 权限提升 | NFC 组件权限提升漏洞                        |
| CVE-2018-9561  | 2019/03/01 | 高危 | 信息泄漏 | Android NFC 信息泄漏漏洞                  |
| CVE-2019-2003  | 2019/03/01 | 高危 | 权限提升 | Android Framework 权限许可和访问控制问题漏洞     |
| CVE-2019-2027  | 2019/04/01 | 严重 | 远程攻击 | Media Framework 中的溢出漏洞              |
| CVE-2019-2034  | 2019/04/01 | 高危 | 权限提升 | NFC 组件权限提升漏洞                        |
| CVE-2019-2044  | 2019/05/01 | 严重 | 远程攻击 | 多媒体服务框架中的远程代码执行漏洞                   |
| CVE-2019-2043  | 2019/05/01 | 中危 | 权限提升 | 设置应用中的权限提升漏洞                        |
| CVE-2019-2092  | 2019/06/01 | 高危 | 权限提升 | DevicePolicyManagerService 权限提升漏洞   |
| CVE-2019-2094  | 2019/06/01 | 严重 | 远程攻击 | NuPlayerCCDecoder 中的越界访问漏洞          |