2017 年度

安卓系统安全性生态环境研究

360 互联网安全中心

2018 年 1 月 12 日

360互联网安全中心

摘　　要

- 此报告数据来源为“360 透视镜”（360 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 80 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 64 个漏洞，涵盖了 Android 系统的各个层面。

- 检测结果显示，截止至 2017 年 12 月，所测设备中 93.94%的 Android 手机存在安全漏洞，有 6.06%的设备完全没有检测出漏洞，安全程度同比上升 1.64%，这一数据刷新了国内安卓系统安全生态情况的最高纪录，同比 2016 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 4.4，比例分别为 38%、28%和 22%，Android 7.0 和 7.1 版本所占比例分别为 3%和 4%，而最新版的 Android 8.0 和 8.1 版本占比几乎为 0%。从结果上看，Android 版本高低和漏洞数量多少并没有严格的线性关系，在高版本系统上（7.0 及以上），漏洞数量明显减少，平均漏洞数有所降低。与上季度相比，用户整体的版本更新和推进变化不大，Android 6.0 依旧是用户量最多的系统，高版本系统 7.0 和 7.1 继续保持缓慢上升趋势；在平均漏洞数方面，以 6.0 版本为分界线，6.0 及以下平均漏洞数量整体保持上升，而 7.0 及以上的平均漏洞数相比上个季度则有所降低。虽然检测的漏洞总案例在继续增加，但高版本系统平均漏洞降低的这种情况与新版本系统中安卓系统安全补丁的普及有很大的关系。

- 用户手机的平均漏洞数量存在比较明显的地域特征，上海、广东、天津等地区的用户手机平均漏洞数量最少，青海、宁夏、甘肃等地区的用户手机漏洞数量相对较多。这一数据的顺序较上一季度略有变化，整体平均漏洞数基本持平。

- 不同性别的用户平均系统版本较上一季度均有所提升，男性用户的手机版本平均比女性用户的手机版本低，女性用户的手机平均漏洞数量比男性用户低。

- 其中 87.4%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 4 个漏洞，占比 18.2%，仅有 12.6%的设备不受浏览器内核漏洞影响。与上一季度相比，浏览器安全情况有较大缓解，通过我们的观测，这与浏览器内核的升级有直接关联，新版本浏览器内核所占比例明显有所增长。

- 安卓手机用户中，约有 46.0%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 14.6%的用户的手机系统版本会保持滞后厂商最新版本 1 到 3 个月，接近 9%的用户会滞后 4 到 6 个月，其余用户会滞后半年以上。其中保持手机系统更新的用户相较上个季度无明显差异，同比 2016 年，也无明显差异。

- 与安卓官方最新更新情况相比，用户手机系统平均滞后了约 11.1 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 4.1 个月。这两项数据上看，安全补丁的更新环比均有所滞后，但整体差距不大。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，就是手机厂商普遍未能实现其定制开发的安卓系统与 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

360互联网安全中心

目　　录

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，各手机厂商若要为采用 Android 系统的各种设备修复安全问题则需投入大量人力物力。

随着各种系统漏洞的不断披露，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能有效修补，攻击大门依旧打开。而 Android 平台之上的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 历时一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 系统上实现了无需申请敏感权限即可检测 Android 系统中存在的漏洞这一核心功能，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 80 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 2017 年 12 月）Android 与 Chrome 安全公告中检出率最高的 64 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。

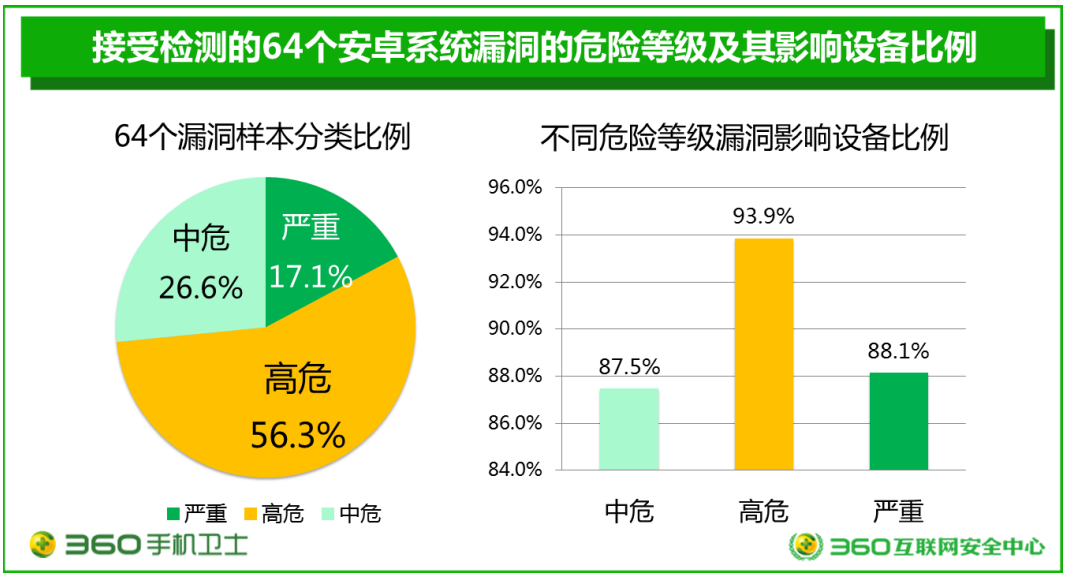
第一章　手机系统安全性综述

一、　系统漏洞的危险等级

此次报告评测的 64 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。即“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，低危漏洞未入选。

在这 64 个漏洞中，按照其危险等级分类，有严重级别漏洞 11 个，高危级别漏洞 36 个，中危级别漏洞 17 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 73.4%。

此次系统安全分析结果显示： 87.5%的 Android 设备受到中危级别漏洞的危害，93.9%的 Android 设备存在高危漏洞，88.1%的 Android 设备受到严重级别的漏洞影响。

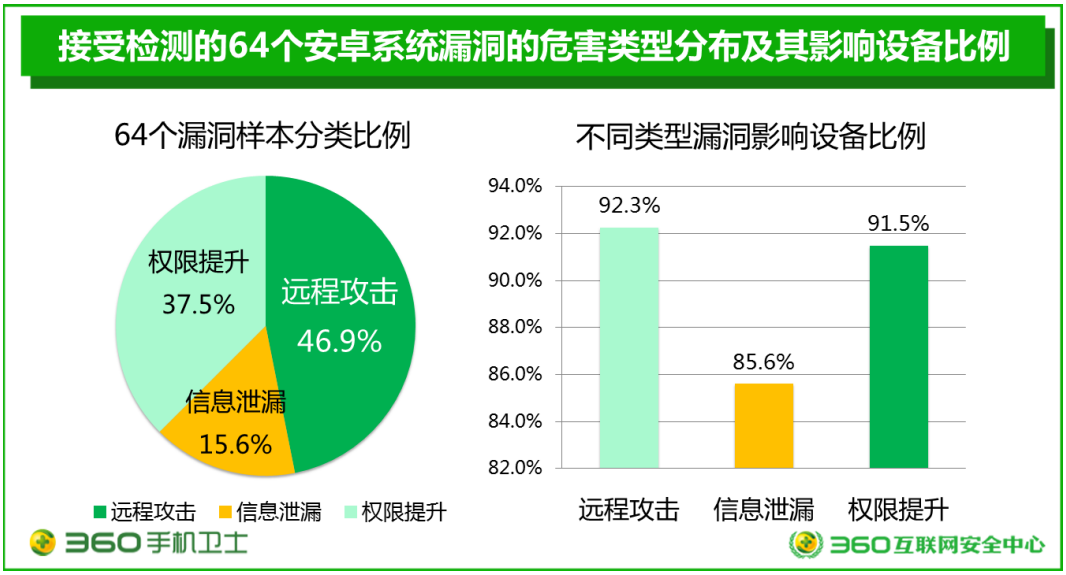


二、　系统漏洞的危害方式

此次报告评测的 64 个系统漏洞，参照 Google 官方对系统漏洞的技术类型分类标准并加以适当合并，按照各漏洞的明显特征分类，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远程对用户的系统进行攻击的漏洞，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 64 个漏洞中，按照其危害方式分类，有远程攻击漏洞 30 个，权限提升漏洞 24 个，信息泄漏漏洞 10 个。

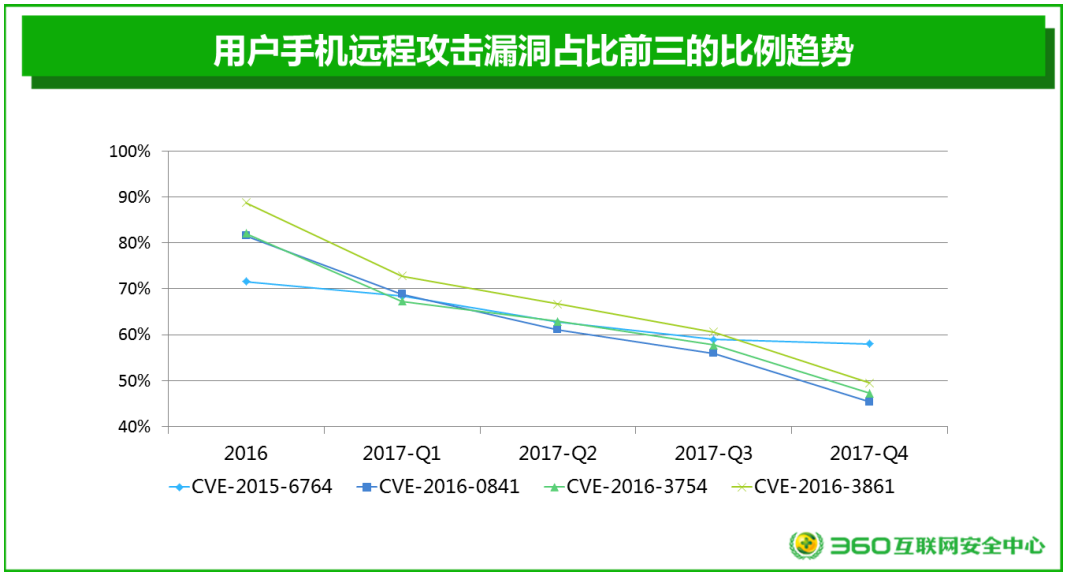
此次系统安全分析结果显示：92.3%的设备存在远程攻击漏洞，91.5%的设备存在权限提升漏洞，85.6%的设备存在信息泄露漏洞。与往期相比，虽然检测漏洞数又有所增加，但影响设备比例有所降低，主要原因为部分设备的厂商大幅度更新手机的安全性，将设备的补丁等级保持与谷歌同步，修复了所有漏洞。



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，其中影响最广泛信息泄露漏洞仍然为 CVE-2016-1677，72.5%的设备都存在这个漏洞，环比上升 1.8%；权限提升漏洞中，CVE-2017-0666 依然影响最广，77.7%的设备均受影响，影响比例下降 5.2%；远程攻击漏洞中，CVE-2015-7555 影响设备依然最多，影响 77.7%的设备，下降 10.5%。而第三季度中我们关注的 CVE-2016-3861 在本季度中影响设备比例已经退出 Top3，取代它的位置是漏洞 CVE-2015-6764，影响 63.0%的设备。

第二季度中 Android 新修复并公开的 CVE-2015-7555 漏洞在本季度中影响设备数量依然十分庞大，同比仅降低了 10.5%，并且预计在未来一段时间仍会如此。CVE-2017-13156 即是 12 月披露的“Janus”漏洞，影响 59.7%的设备。

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，为此我们统计了每期报告中远程攻击漏洞排名 Top3 的趋势变化，结果如下图所示。



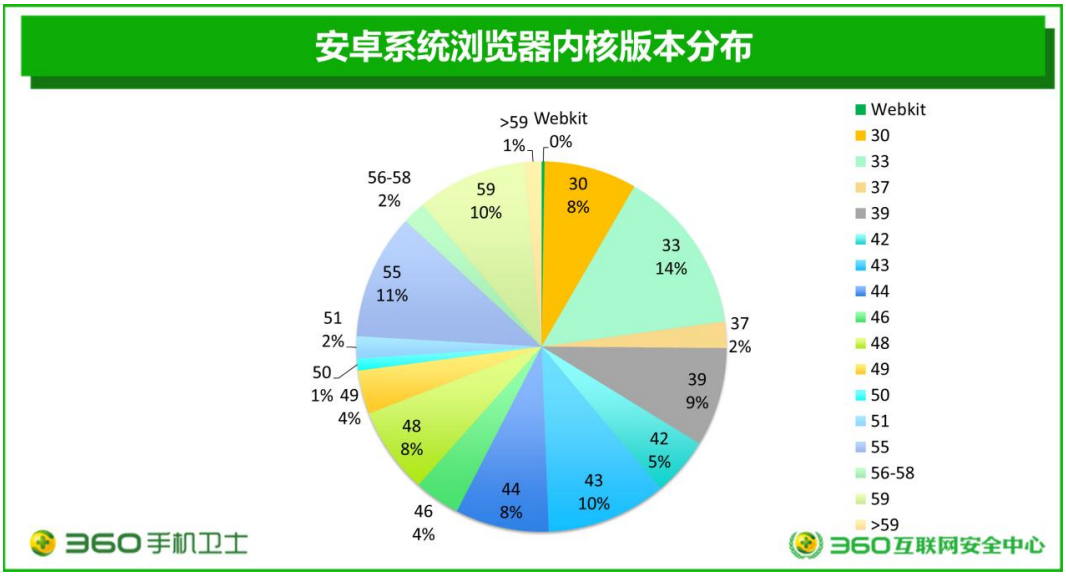
远程攻击漏洞整体呈下降趋势，但是受漏洞影响的设备依旧保持在较高比例，4 成以上的用户手机仍然处于被远程攻击的风险之中，安全形势并不乐观。

三、 系统浏览器内核的安全性

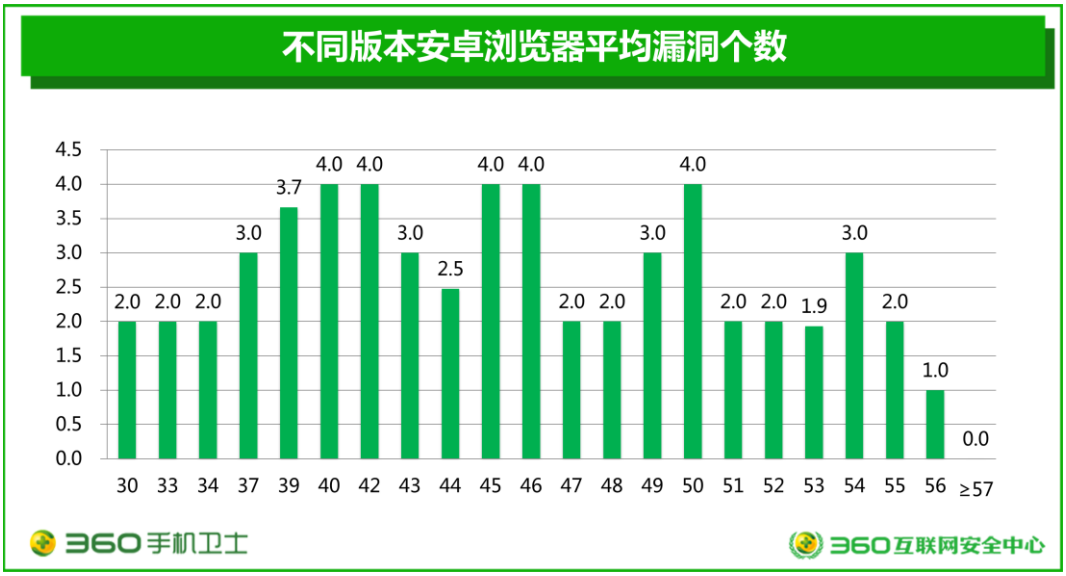
系统浏览器内核是用户每日使用手机时接触最多的系统组件，不仅仅是指用户浏览网页的独立浏览器，实际上，许多安卓应用开发者考虑到开发速度、保障不同设备之间的统一性等因素，会使用系统提供的浏览器内核组件。因而用户在每日的手机使用中，大多会直接或间接地调用了系统浏览器内核。

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)。

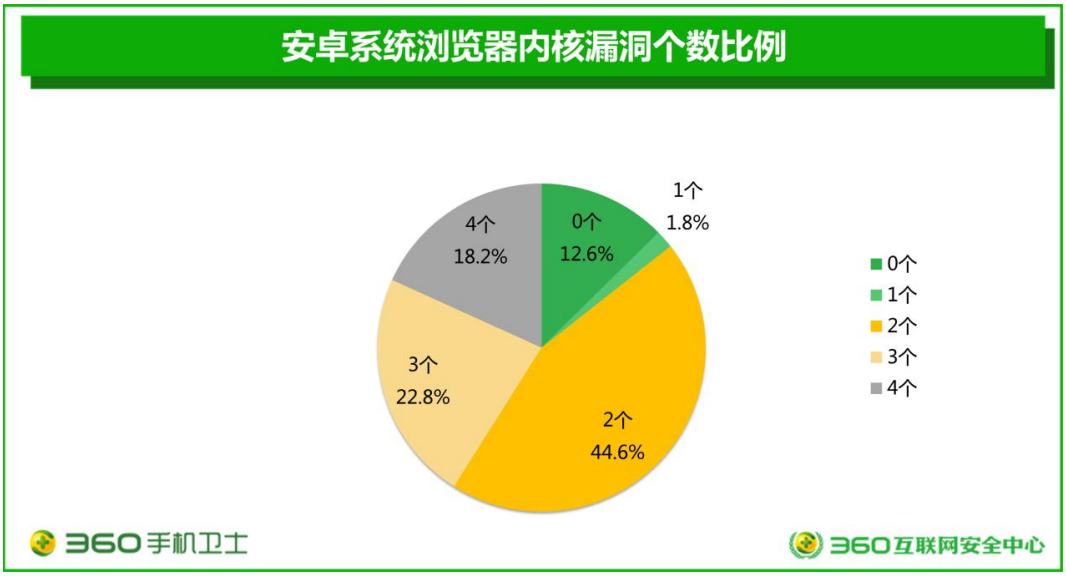
在统计的样本中，其中 Webkit 内核版本由于其版本较为一致，故在示意图中仅占一块，其余为 Chrome 内核的不同版本。本季度 Webkit 所占比重几乎为 0%，较上季度降低 9%。截止至本季度，当前 Google 发布的 Android 平台 Chrome 稳定版的内核的最新版本为 Chrome 60，而在此次检测中有 1%的用户将自己手机中的浏览器内核升级至最新。而从图中可以看出，Chrome 内核版本大于等于 55 的设备占 24%。对比上一季度的数据，版本大于 50 的设备比例有所增长，从 18%增至 27%。在此次检测中，并且最新版本 60 在国内用户之中占比 1%，同比上季度增长 0.91%，说明国内厂商有更新浏览器内核的举措。总的来说，浏览器内核整体版本有所跟新推进，国内安卓生态圈中对浏览器内核的更新进度相对有所增强，但仍存在严重的更新滞后问题，第二节远程攻击漏洞中跻身 Top3 的 CVE-2015-6764，即是浏览器内核漏洞，足以说明这一点。



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 Webview 版本平均漏洞数量，其中内核版本在 Chrome 46 以下的版本中漏洞数量明显高于 Chrome 47 以上版本，Chrome 55 以上版本漏洞数量相对最少。从图中可以看出较新版本浏览器内核漏洞数量相对较少，其中 Chrome 57 版本及以上的设备平均漏洞检出情况则为 0。以上数据充分说明保持最新版本的浏览器内核可以十分有效增强手机浏览器内核的安全性。

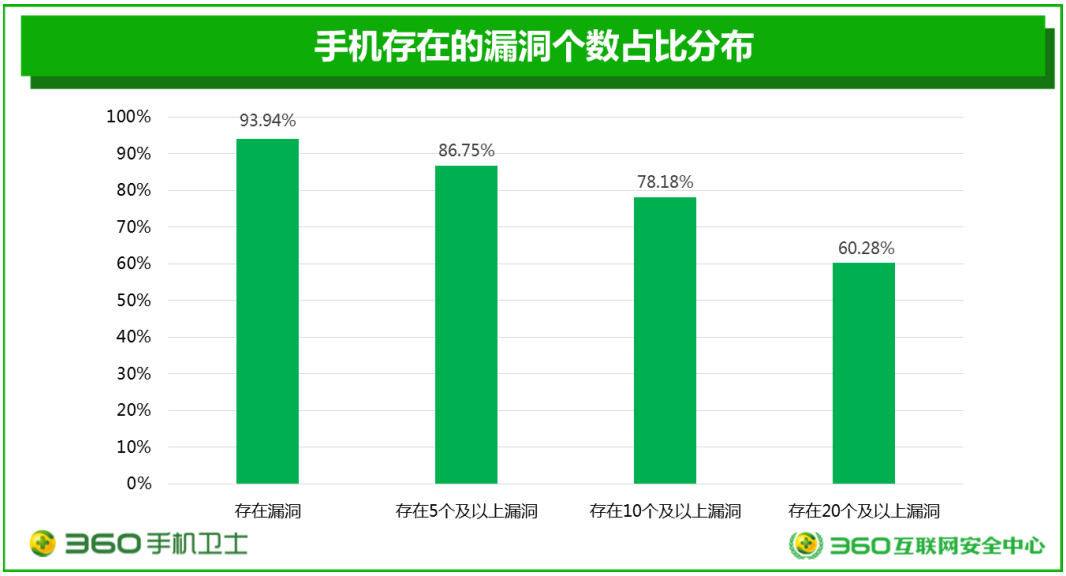


浏览器内核漏洞多数可通过远程方式利用，因而对于用户的手机安全危害较大。安卓系统浏览器内核漏洞的分布情况如下图所示。其中 87.4%的设备存在至少一个浏览器内核漏洞，18.2%的设备同时存在 4 个浏览器内核漏洞，为漏洞数量最多的设备。有 12.6%的设备不受这些漏洞影响。较上一季度，浏览器安全情况有所上升，但上升比例不大。整体来看浏览器安全状态有所缓解，浏览器内核版本的更新所带来的效果十分显著，但老旧设备的升级情况无明显好转，用户依然暴露在浏览器漏洞的威胁之中。



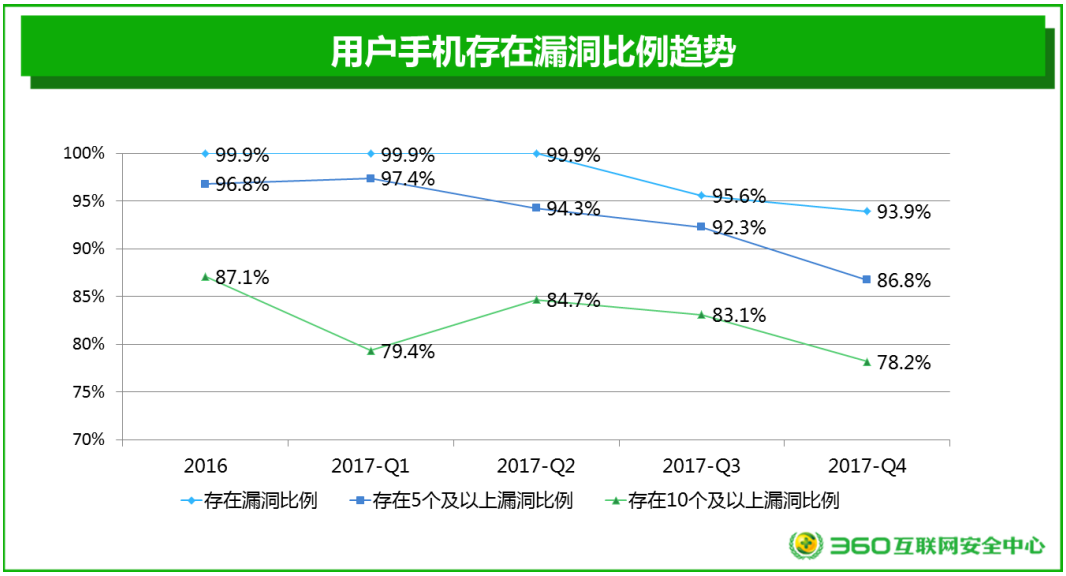
四、 系统漏洞的数量分布

为了研究用户手机中漏洞数量的分布规律和对用户手机中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 64 个已知漏洞，有 93.94%的设备存在至少一个安全漏洞，漏洞最多的设备同时包含有 49 个安全漏洞。这一数据较上一季度 95.58%的比例降低幅度不大，其他漏洞个数的比例情况与上一季度相比整体有所降低，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 2016 年到 2017 年的漏洞数量比例分布及趋势，结果如下图所示。

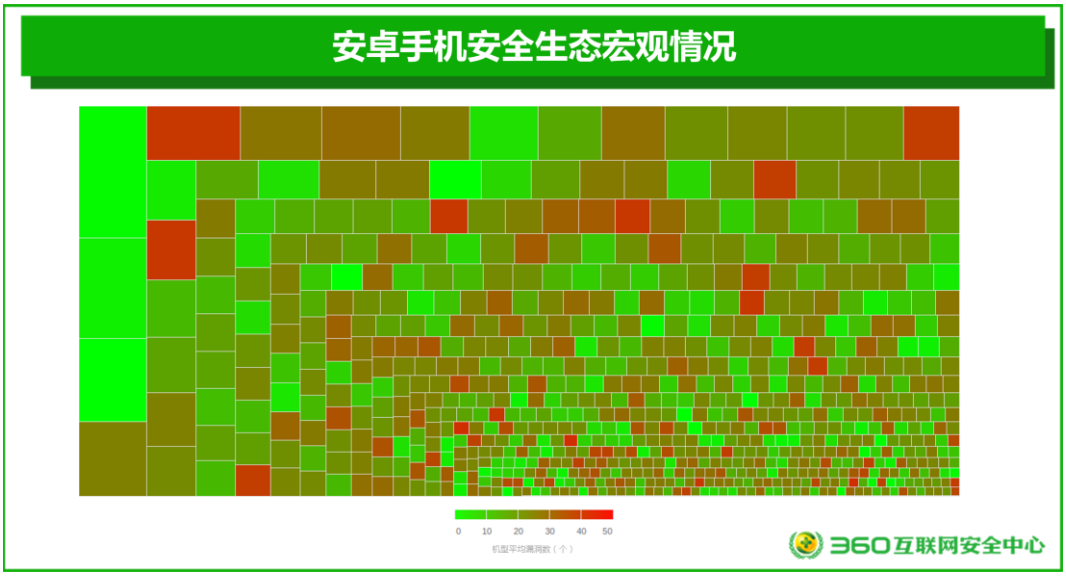


可以发现，手机存在漏洞的比例，整体呈下降的趋势。2017 年第一季度，10 个及以上漏洞的比例下降幅度增加，跟该季度较高比例的系统更新有直接关系，第五章第二节也会有相应的数据反映这一现象。2017 年第一到第二季度漏洞比例有所上升，与这期间新增漏洞检测样本数量有关，这也说明一旦加大检测力度，用户手机整体的安全形势将会表现的更加严峻。

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情况就会有明显的提升。虽然国内厂商在不断地对安卓设备进行安全更新，但是安全漏洞也在层出不穷，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，较为安全的绿色方块数量依旧较少，整体安全情

况依旧比较严峻。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，部分厂商则将系统更新至与安卓官方同步（2017-12），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

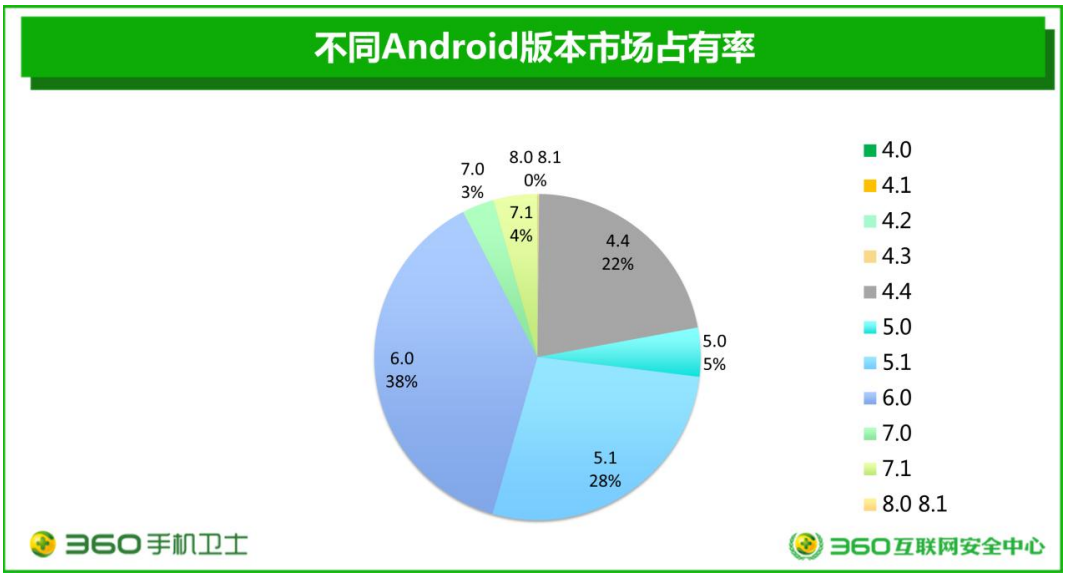
一、 各系统版本漏洞情况

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。

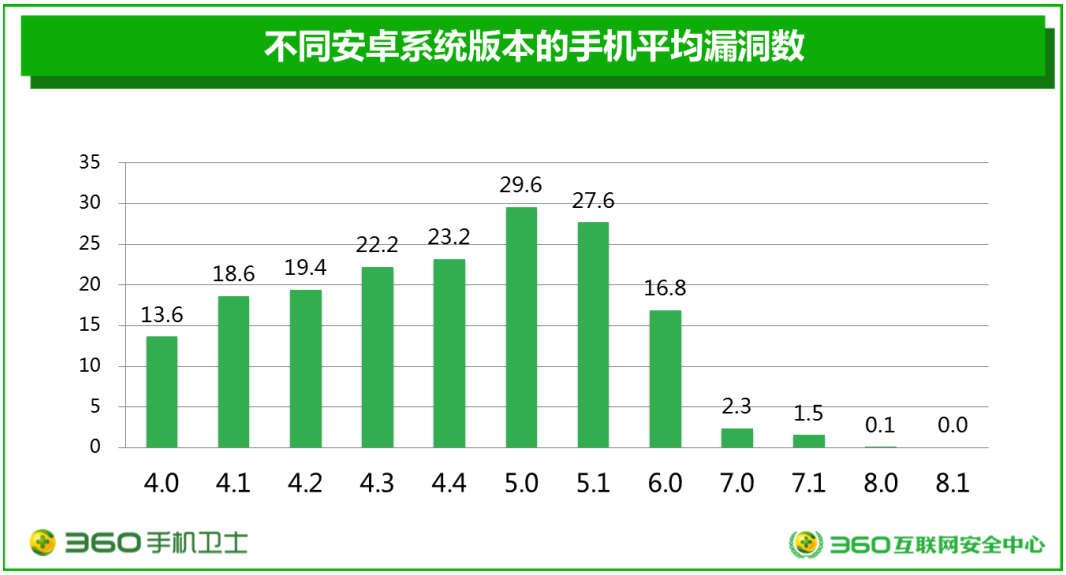
为了研究不同版本的安卓系统的安全性，我们统计了样本手机所使用的安卓版本分布，并进一步对这些不同的版本的漏洞数量进行了统计分析。

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 4.4，比例分别达到 38%、28%和 22%，而高版本中 Android 7.0 和 7.1 版本所占比例分别为 3%和 4%，Android 8.0 及以上接近为 0。

与上一季度相同，Android 6.0 依旧成为最流行的系统版本，与历史进程和我们的预期均相符。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 60%的比例。Android 7.0 和 7.1 的比例有小幅度上升，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，其中包括引入的隐私敏感权限动态管理功能，而这在一定程度上极大的增强了用户手机隐私的安全性。目前最新的系统为 Android 8.0，其中引入了一项叫做 Project Treble 的功能，在未来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。但由于新系统、新设备无法第一时间大范围更新，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 6.0 以上系统则更为安全，平均漏洞数量急剧降低。其中比较新的 Android 7.0 和 7.1 的系统中，平均漏洞数较上一季度有所降低，这主要是由于新版本的系统中安全补丁推送已经较为普及，厂商对于新版本系统的推送积极度有所上升。



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，而 Android 4.4 发布距今已经过去了 3 年的时间，因而相对版本越老的 Android 系统因为不支持较新的功能而可能不存在相应的漏洞。Android 5.0 以上版本，随着系统版本升高，漏洞数量急剧减少。

环比上季度的数据，除 7.0 和 7.1 外，其余版本系统的平均漏洞数均有所增加，这是由于本季度又新修复和公开了一些漏洞，而这些漏洞中有些漏洞影响范围十分广泛。

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次加固。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 系统中谷歌工程师对 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，攻击者也无法在别的进程空间内执行代码；并且在整个 Media Server 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。在最新的 Android 8.0 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。

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。

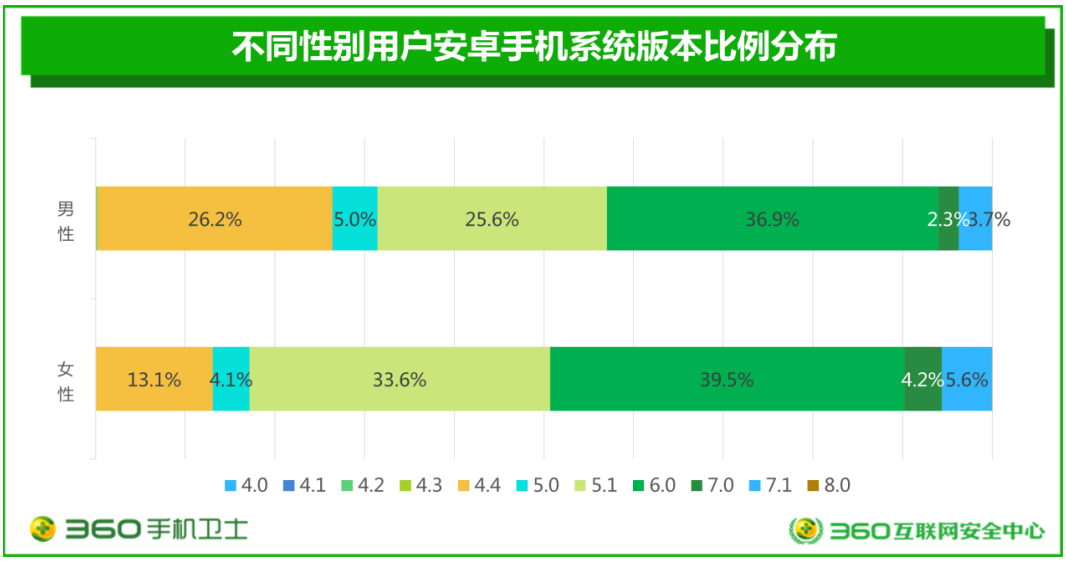
下图为各省份平均每台手机漏洞数量，数值越大，说明该地域安卓手机的安全性相对越低、越不安全；数字越小，则代表该地域安卓手机的安全性越高。手机安全性最低的前三名为青海、宁夏、甘肃，平均每台手机拥有漏洞数分别为 22.8、22.6、22.1 个。而安全性最高的前三名为上海、广东、天津，平均每台手机拥有漏洞数 18.7、19.4、19.6。大致上，经济越发达的地区，用户所使用的手机的平均漏洞数量越少，手机安全性相对越高。

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。

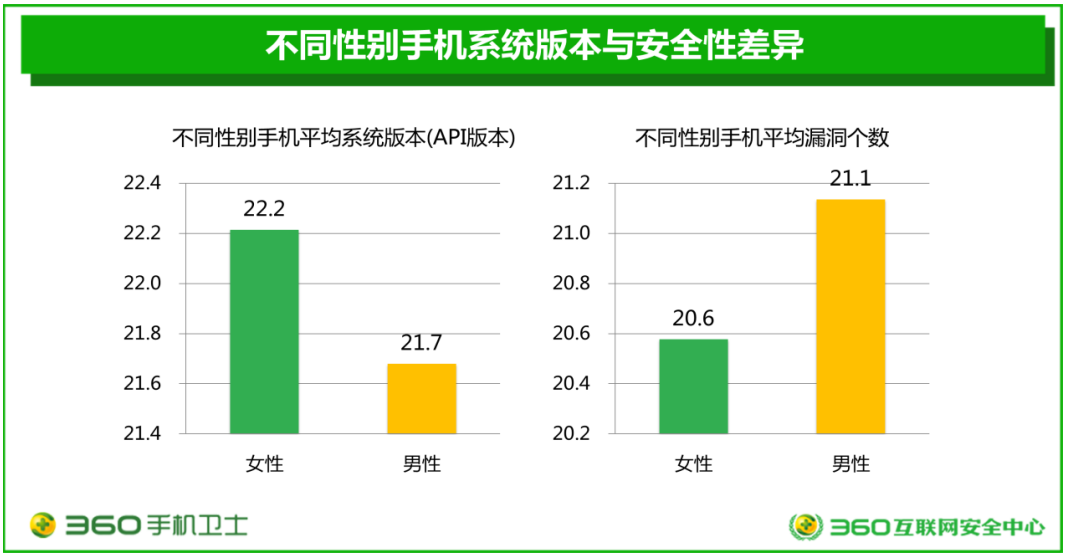
第四章　手机系统安全性与用户性别的相关性

由于性别上天生的性格、喜好等的差异，不同性别的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与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：男性使用系统版本大于或等于 5.1 的手机的比例远低于女性用户，包括各版本的比例中，男性用户使用的比例也明显低于女性用户；而男性用户中使用系统版本低于 5.1 的比例要远高于女性用户所占的比例，包括各版本的比例中，男性用户使用的比例也明显高于女性用户。即女性用户中，使用新版本手机的比例明显高于男性，这一结论在上述数据中，以 6.0 为界限统计的宏观角度和以不同安卓小版本单独统计的微观角度都成立。



在不同性别的用户手机的所存在的漏洞情况如上图所示。我们可以看到女性手机的平均系统版本数值约为 22.2 (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)，即平均使用的版本号接近 Android 5.1，而男性使用的平均版本号为 21.7，平均使用的 Android 版本号也接近 5.1。

对比上季度的统计数据，男性和女性的平均系统版本均有所提升，其中女性平均版本号提升了 0.4，男性则为 0.7。

在此次统计中，我们发现，女性手机平均版本比男性要高，且均大于等于 5.1，而平均漏洞数女性手机所存在的漏洞数量也是低于男性。这与上面我们分析的漏洞数量与系统新旧不是简单的线性关系有关，并且和我们上述对于不同版本的安卓系统的漏洞数中的高于 5.1 版本的系统的平均漏洞个数开始递减的结论保持一致。

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。

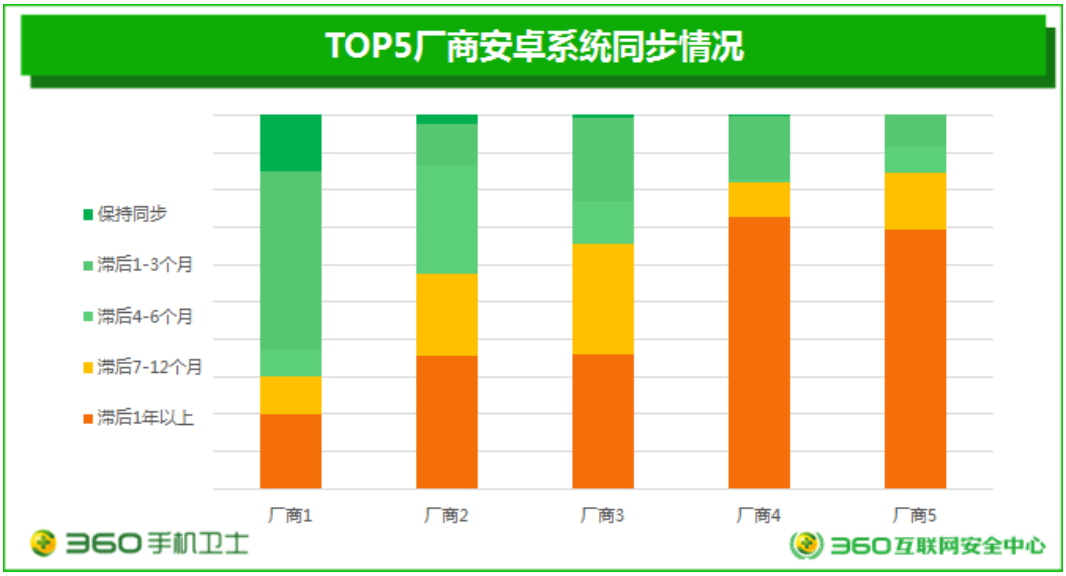
在 Android 系统中，存在一个名为“Android 安全补丁级别”的字段，它是谷歌公司向第三方安卓手机厂商推送的一个 Android 安全补丁的日期号，旨在为安卓设备的已知漏洞的修复情况做一个简单的说明。当前谷歌对于 Android 4.4 及其上版本号的安卓系统会定期推送更新，如果厂商遵循谷歌公司的建议正确打入补丁，那么手机中显示的安全补丁级别日期越新，手机的安全情况就相对越安全。

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。

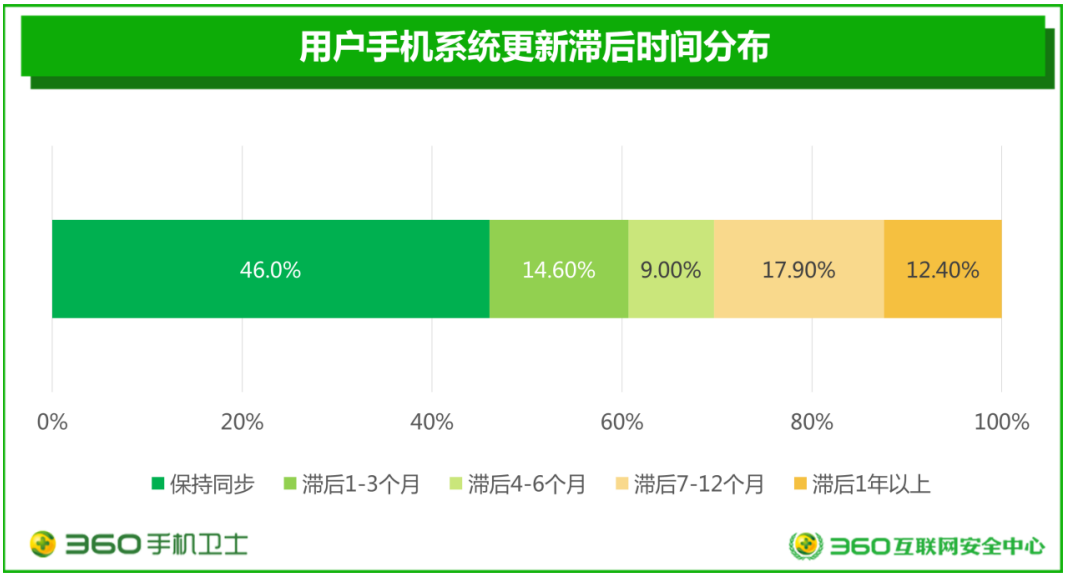
下图为各厂商手机中实际存在的安全补丁级别情况，该情况是将各厂商现存手机中实际补丁日期与谷歌官方最新版本（2017 年 12 月）版本对比，综合安全补丁级别最高、最新的手机品牌前 5 名。图中绿色方块面积越大，说明该厂商的手机补丁级别相对越高，漏洞修复相对越及时；相反，如果黄色和橙色面积越大，则说明补丁级别越低，漏洞修复越滞后。



图中我们可以看出，在及时推送安全补丁级别方面，TOP5 的厂商在本季度的检测结果显示较好，而且在本季度的调研中这五个厂商均有保持与谷歌最新安全补丁同步的更新提供，这也显示了厂商对于用户手机中安全补丁等级的逐步重视。

二、 用户主动升级意愿

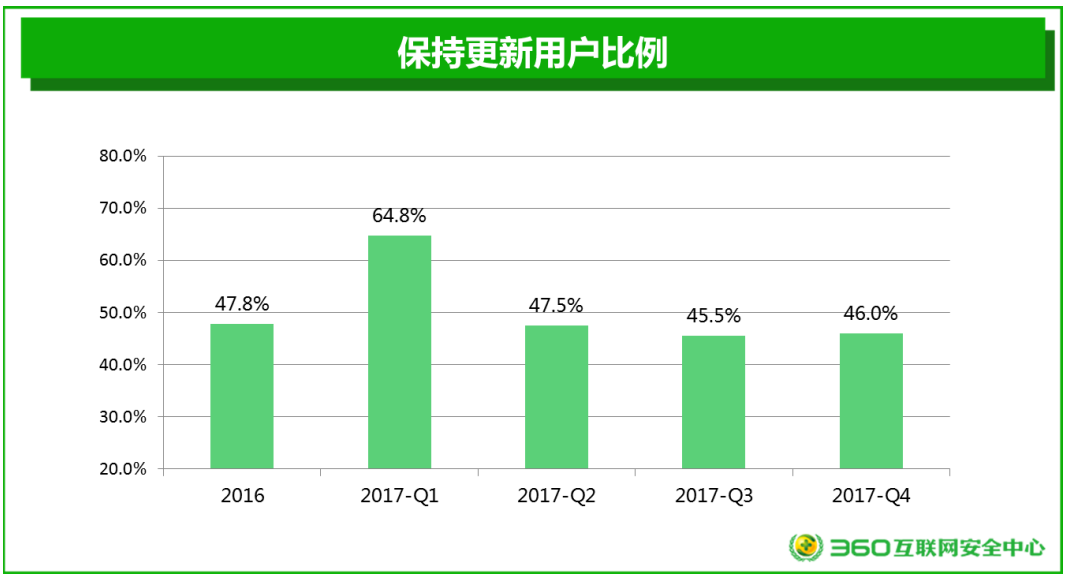
此次研究中，为了探究用户主动升级系统的意愿，我们统计了不同厂商、不同机型、不同安全补丁级别的分布情况。此统计为在每个机型中，观察用户是否主动保持这个厂商对此机型提供最新版本。



整体上，可以明显发现近一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 46.0%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。

但是仍有 14.6%的用户的系统版本滞后厂商最新版本 1-3 个月，大约 9.0%的用户手机版本滞后 4-6 个月，约 17.9%的用户手机版本滞后半年以上，有 12.4%的用户手机版本滞后官方最新版本达一年以上，而这些用户将比保持系统更新的用户更多地暴露在更多的漏洞与更大的攻击风险之下。

我们还统计了近两年来用户与手机厂商保持更新的比例变化情况，如下图所示。



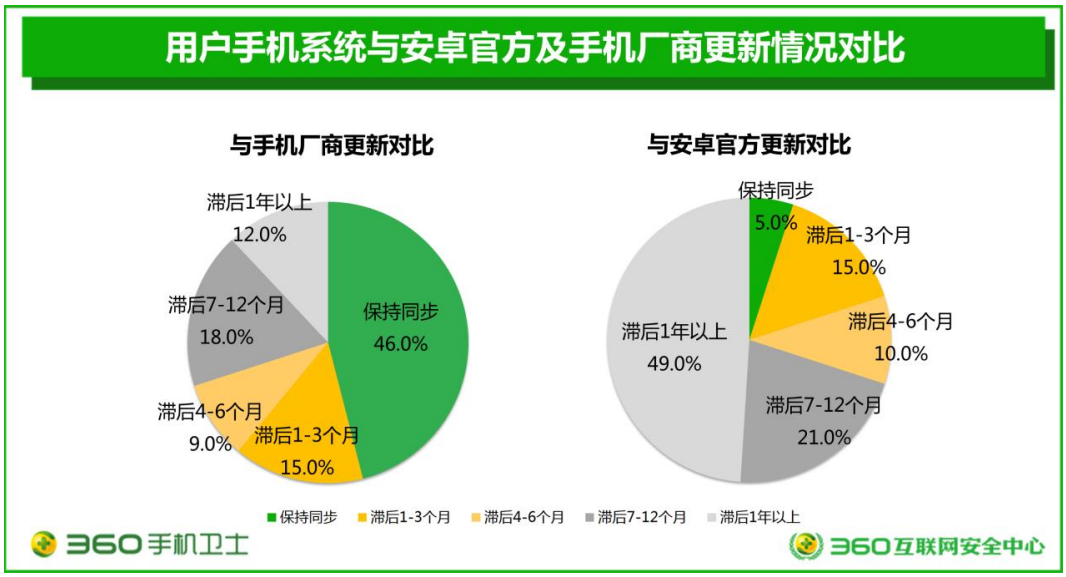
整体来说，近半用户还是会愿意保持系统更新至最新版本，但是保持更新的比例并没有呈现上升趋势，而且更新比例仍然偏低，一半以上的用户手机处于高风险状态。

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。

从移动网络安全角度来看，我们建议手机厂商在不影响用户体验的基础上，尽量为手机用户提供系统漏洞安全补丁方面的更新，以保护用户移动安全不受影响。

三、 漏洞修复综合分析

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 6 成以上的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 5%，滞后时间小于 3 个月的用户也只有近 20%，较上季度比例均有所下降。

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情况相比，用户的手机系统平均滞后了约 11.1 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 4.1 个月，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　典型手机系统高危漏洞实例

经过上述对 Android 系统漏洞的研究，我们可以看出仍然存在大量未升级至新版本系统和未打补丁的设备正在被使用，这些与安全更新脱节的现象直接导致用户手机暴露于各种漏洞的威胁之下，可造成用户的隐私、财产安全。

下面我们以近期著名的“Janus”漏洞作为案例，分析漏洞对 Android 用户的实际威胁：

一、 漏洞简介

Android 12 月安全公告中披露了一个名为“Janus”的漏洞(编号：CVE-2017-13156)，攻击者可以利用该漏洞绕过 Android 系统的 signature scheme V1 签名机制，直接对 App 进行篡改。由于签名和验证机制是 Android 系统整体安全机制建立的最基础部分，利用该漏洞可以绕过整个 Android 系统的安全机制。基于 signature scheme V1 签名机制的 App 在 Android 5.1 到 8.0 系统均受“Janus”漏洞影响。

二、 漏洞危害

如果攻击者将植入恶意代码的伪造的 App 投放到 Android 应用市场，就可替代原有的 App 而提供下载、更新，造成的可能后果如下：

1. 用户隐私泄露，如通信、社交类 APP 的聊天记录、图片、通信录等。

2. 用户财产损失，如窃取金融类 App 的支付密码、钱包密码、token 等; 监听、拦截用户的输入，使用欺诈手段，诱骗用户进行输入密码、转账行为。

3. 利用该漏洞可以更新 Android 的系统 APP，从而获得更高的系统权限，达到更高级的攻击效果，如远程控制手机等。

三、 漏洞影响

根据第一章第二节数据显示，受此漏洞影响的设备比例为 59.7%，表明有近 6 成的用户手机仍然存在被此漏洞攻击的风险。

附录

此次分析中所检测的 64 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 组件中的远程代码执行漏洞
CVE-2016-0841	2016/02/26	严重	远程攻击	MetadataRetriever 组件中的远程代码执行漏洞
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代码执行漏洞
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	媒体服务中的远程代码执行漏洞
CVE-2017-0589	2017/05/01	严重	远程攻击	媒体服务中的远程代码执行漏洞
CVE-2015-7555	2017/05/05	严重	远程攻击	GIFLIB 远程代码执行漏洞
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-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 引擎的远程代码执行漏洞
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	蓝牙组件中的远程代码执行漏洞
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	蓝牙组件中的远程代码执行漏洞
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代码执行漏洞
CVE-2016-3744	2016/07/01	高危	远程攻击	蓝牙组件中的远程代码执行漏洞
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 中的远程代码执行漏洞
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-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披露漏洞
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代码执行漏洞