





2017 中国互联网安全大会 China Internet Security Conference

万均皆变 人是安全的尺度

Of All Things Human Is The Measure

来自N-Day的安全威胁 揭秘安卓系统安全生态

大木 360Alpha Team成员 安全研究员





关于我们

360 Alpha Team(阿尔法团队)隶属于奇虎360公司,致力于Android系统漏洞、Chrome浏览器安全以及Android系统安全生态的研究。

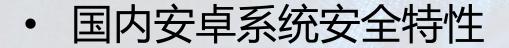
团队曾发现60余个谷歌漏洞而获得20余次谷歌致谢, 赢得4次世界黑客大赛 (Pwn2Own 2015 Mobile, Pwn2Own 2016, Pwn0Rama 2016, PwnFest 2016)。

发布了中国第一个安卓系统漏洞检测工具 "透视镜"





目录



- 安卓系统上漏洞扫描的原理和细节
- 真实的安卓系统安全生态
- 总结

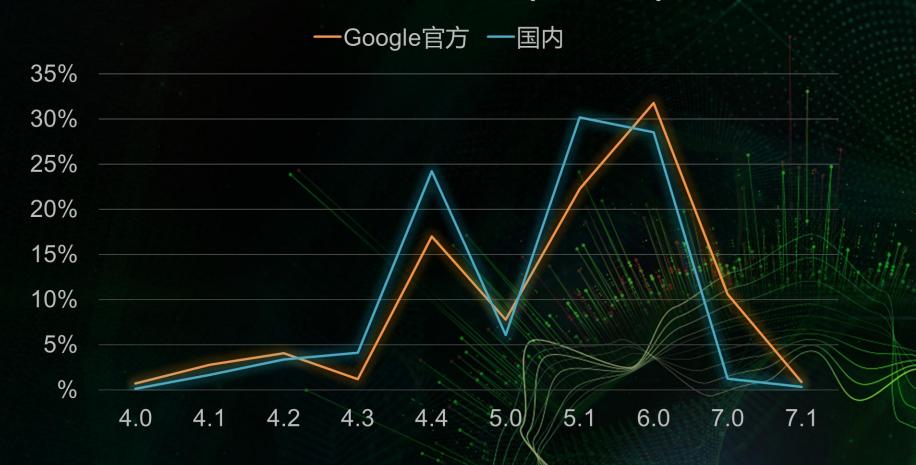


国内安卓系统的安全特性





国内外安卓版本分布对比(2017.07)

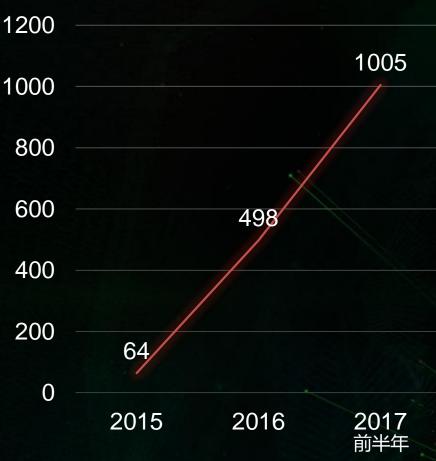


安卓漏洞ODay 与 N-Day









而在今天看来,这些都变成了N-Day

- 缺乏高效的统一更新机制
- 更新维护周期短
- 设备服役周期长

为什么恶意软件多选择N-Day?

性价比更高

- ✓ 研发0Day利用成本高
- ✓ 维护成本高

安卓漏洞检测技术





第三方应用可调用的漏洞

- 利用PoC/Exp
- 调用漏洞关键函数

第三方应用无法调用的漏洞

• 依据补丁/漏洞的特征进行静态特征匹配

安卓漏洞检测细节





在检测Androi系统漏洞时注意的细节

- 全程无害,避免检测引发系统崩溃
- 保证稳定,避免检测应用自身崩溃
- 范围广泛,无需将设备Root
- 无需权限,避免涉及隐私问题





如何检测产生系统宣全的生态情况?

检测所选择的部分漏洞





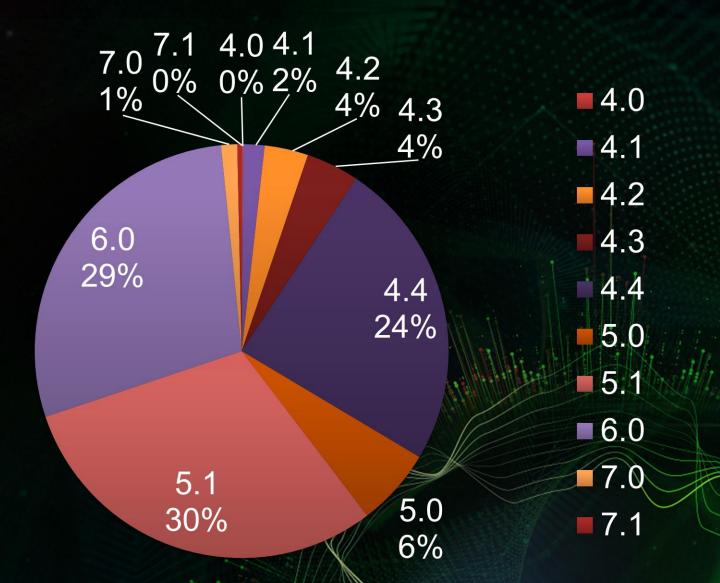
CVE-2016-0838 2016/01/12 严重 远程攻击 Sonivox组件中的远程代码执行漏洞 CVE-2016-0841 2016/02/26 严重 CVE-2016-3754 2016/07/01 高危 远程攻击 媒体服务进程中的远程担控 CVE-2016-2430 2016/03/25 严重 CVE-2016-6754 2016/10/03 高危 权限提升 照相机应用中的权限提升 CVE-2016-2463 2016/06/01 严重 CVE-2016-6754 2016/11/01 高危 远程攻击 BadKernel漏洞 CVE-2016-3861 2016/09/01 严重 CVE-2016-6710 2016/11/03 高危 信息泄漏 下载管理器中的信息泄漏洞 CVE-2016-3861 2016/12/05 严重 CVE-2016-9651 2016/12/01 高危 远程攻击 PwnFest2016 Chrome v8 CVE-2017-0471 2017/03/01 严重 CVE-2017-0386 2017/01/03 高危 校限提升 原体联升 PwnFest2016 Chrome v8 CVE-2015-0559 2017/05/01 严重 CVE-2017-0421 2017/02/01 高危 远程攻击 PwnFest2016 Chrome v8 CVE-2015-3849 2015/01/27 高危 CVE-2016-2426 2016/06/01 高危 远程攻击 中危 远程攻击	
CVE-2015-1805 2016/03/18 严重 CVE-2016-3915 2016/07/01 高危 反程攻击 無体服务近程中的边程指示 CVE-2016-2430 2016/03/25 严重 CVE-2016-6754 2016/11/01 高危 权限提升 照相机应用中的权限提升 CVE-2016-3861 2016/09/01 严重 CVE-2016-6710 2016/11/03 高危 信息泄漏 下载管理器中的信息泄漏 CVE-2016-5195 2016/12/05 严重 CVE-2017-0471 2017/03/01 严重 CVE-2017-0386 2017/01/03 高危 信息泄漏 下载管理器中的信息泄漏》 CVE-2017-0471 2017/03/01 严重 CVE-2017-0421 2017/02/01 高危 信息泄漏 安卓框架中的信息泄漏洞 CVE-2017-0589 2017/05/05 严重 CVE-2017-0412 2017/02/01 高危 权限提升 系统框架权限许可和访问 CVE-2015-1532 2015/08/13 高危 CVE-2016-4658 2017/06/01 高危 远程攻击 Iibxml2中的远程长行洞 CVE-2015-6764 2015/11/18 高危 CVE-2016-2426 2016/04/02 中危 信息泄漏 Chrome V8 decodeURI 信 CVE-2016-2416 2016/02/26 高危 CVE-2016-1688	
CVE-2015-1805 2016/03/18 严重 CVE-2016-3915 2016/10/03 高危 权限提升 照相机应用中的权限提升 CVE-2016-2430 2016/06/01 严重 CVE-2016-6754 2016/11/01 高危 远程攻击 BadKernel漏洞 CVE-2016-3861 2016/09/01 严重 CVE-2016-6710 2016/11/03 高危 信息泄漏 下载管理器中的信息泄漏 CVE-2016-5195 2016/12/05 严重 CVE-2017-0471 2017/03/01 严重 CVE-2017-0386 2017/01/03 高危 校限提升 PwnFest2016 Chrome v8 CVE-2017-0589 2017/05/01 严重 CVE-2017-0421 2017/02/01 高危 校限提升 系统框架中的信息泄漏洞 CVE-2015-7555 2017/05/05 严重 CVE-2017-0412 2017/02/01 高危 校限提升 系统框架权限许可和访问 CVE-2015-3849 2015/08/13 高危 CVE-2016-4658 2017/06/01 高危 远程攻击 中の2017 远程执行漏洞 CVE-2015-6771 2015/11/18 高危 CVE-2016-4658 2017/06/01 高危 远程攻击 CVE-2016-2426 2016/04/02 中危 信息泄漏 安卓框架中的远程攻击 CVE-2016-2426	·····································
CVE-2016-2430 2016/03/25 严重 CVE-2016-6754 2016/11/01 高危 远程攻击 BadKernel漏洞 CVE-2016-3861 2016/06/01 严重 CVE-2016-6710 2016/11/03 高危 信息泄漏 下载管理器中的信息泄漏洞 CVE-2016-3861 2016/12/05 严重 CVE-2016-9651 2016/12/01 高危 远程攻击 PwnFest2016 Chrome v8 CVE-2017-0471 2017/03/01 严重 CVE-2017-0386 2017/01/03 高危 权限提升 libnl库中的权限提升漏洞 CVE-2017-0589 2017/05/01 严重 CVE-2017-0421 2017/02/01 高危 右息泄漏 安卓框架中的信息泄漏洞 CVE-2015-7555 2017/05/05 严重 CVE-2017-0412 2017/02/01 高危 板限提升 系统框架权限许可和访问 CVE-2015-1532 2015/01/27 高危 CVE-2016-4658 2017/06/01 高危 远程攻击 pwn2own2017 远程执行漏洞 CVE-2015-6764 2015/11/18 高危 CVE-2016-2426 2016/04/02 中危 信息泄漏 安卓框架中的信息泄漏洞 CVE-2016-2412 2016/02/26 高危 CVE-2016-1677 2016/05/25 中危 信息泄漏 <	
CVE-2016-2463 2016/06/01 严重 CVE-2016-6710 2016/11/03 高危 信息泄漏 下载管理器中的信息泄漏 CVE-2016-3861 2016/09/01 严重 CVE-2016-9651 2016/12/01 高危 远程攻击 PwnFest2016 Chrome v8 CVE-2017-0471 2017/03/01 严重 CVE-2017-0386 2017/01/03 高危 村限提升 IibnI库中的权限提升漏洞 CVE-2017-0589 2017/05/05 严重 CVE-2017-0421 2017/02/01 高危 有息泄漏 安卓框架中的信息泄漏漏洞 CVE-2015-7555 2017/05/05 严重 CVE-2017-0412 2017/03/29 高危 远程攻击 pwn2own2017 远程执行洞 CVE-2015-1532 2015/01/27 高危 CVE-2016-4658 2017/06/01 高危 远程攻击 libxmI2中的远程代码执行洞 CVE-2015-3849 2015/08/13 高危 CVE-2016-4658 2016/04/02 中危 信息泄漏 安卓框架中的信息泄漏洞 CVE-2015-6764 2015/12/01 高危 CVE-2016-2426 2016/04/02 中危 信息泄漏 Chrome V8 decodeURI 信息泄漏 CVE-2016-2412 2016/02/26 高危 CVE-2016-1688 2016/05/25 中危 远程	
CVE-2016-3861 2016/09/01 严重 CVE-2016-5195 2016/12/05 严重 CVE-2017-0471 2017/03/01 严重 CVE-2017-0589 2017/05/01 严重 CVE-2015-7555 2017/05/05 严重 CVE-2015-1532 2015/01/27 高危 CVE-2015-3849 2015/08/13 高危 CVE-2016-6764 2015/11/18 高危 CVE-2016-2412 2016/02/26 高危 CVE-2016-2426 2016/05/25 中危 信息泄漏 安卓框架中的信息泄漏漏 CVE-2016-2412 2016/02/26 高危 CVE-2016-1677 2016/05/25 中危 這程攻击 Chrome V8 decodeURI 信息泄漏 CVE-2016-2416 2016/03/01 高危 CVE-2016-1688 2016/05/25 中危 远程攻击 Chrome V8 decodeURI 信息泄漏 CVE-2016-0826 2016/03/01 高危 CVE-2016-1688 2016/05/25 中危 远程攻击 Chrome V8 decodeURI 信息泄漏 CVE-2016-0830 2016/03/01 高危 CVE-2016-3760 2016/06/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0837 2016/03/	
CVE-2016-5195 2016/12/05 严重 CVE-2017-0386 2017/01/03 高危 权限提升 libnl库中的权限提升漏洞 CVE-2017-0471 2017/03/01 严重 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-2015-7555 2017/05/05 严重 CVE-2017-0412 2017/03/29 高危 反限提升 系统框架权限许可和访问 CVE-2015-1532 2015/08/13 高危 CVE-2016-4658 2017/06/01 高危 远程攻击 pwn2own2017 远程执行漏 CVE-2015-3849 2015/08/13 高危 CVE-2016-4658 2017/06/01 高危 远程攻击 libxml2中的远程代码执行流 CVE-2015-6764 2015/11/18 高危 CVE-2016-2426 2016/05/25 中危 信息泄漏 安卓框架中的信息泄漏漏流 CVE-2016-2412 2016/02/26 高危 CVE-2016-1688 2016/05/25 中危 远程攻击 Chrome V8 decodeURI 信息泄漏 CVE-2016-2416 2016/02/26 高危 CVE-2016-1688 2016/05/25 中危 远程攻击 Chrome V8 引擎的信息泄漏 CVE-2016-0826 2016/03/01 高危 CVE-2016-3832 2016/08/01 中危	
CVE-2017-0471 2017/03/01 严重 CVE-2017-0421 2017/02/01 高危 信息泄漏 安卓框架中的信息泄漏漏 CVE-2017-0589 2017/05/05 严重 CVE-2017-0412 2017/02/01 高危 权限提升 系统框架权限许可和访问 CVE-2015-7555 2017/05/05 严重 CVE-2017-0412 2017/03/29 高危 远程攻击 pwn2own2017 远程执行源 CVE-2015-1532 2015/01/27 高危 CVE-2016-4658 2017/06/01 高危 远程攻击 pwn2own2017 远程执行源 CVE-2015-3849 2015/08/13 高危 CVE-2016-4658 2017/06/01 高危 远程攻击 libxml2中的远程代码执行源 CVE-2015-6764 2015/11/18 高危 CVE-2016-2426 2016/04/02 中危 信息泄漏 安卓框架中的信息泄漏漏 CVE-2015-6771 2015/12/01 高危 CVE-2016-2426 2016/05/25 中危 信息泄漏 Chrome V8 decodeURI 信息泄漏 CVE-2016-2416 2016/02/26 高危 CVE-2016-1688 2016/05/25 中危 坂限提升 安卓框架界面中的权限提升 CVE-2016-0826 2016/03/01 高危 CVE-2016-3832 2016/08/01 中危 权限提升	
CVE-2015-7555 2017/05/05 严重 CVE-2017-5053 2017/03/29 高危 远程攻击 pwn2own2017 远程执行漏 CVE-2015-1532 2015/01/27 高危 CVE-2016-4658 2017/06/01 高危 远程攻击 libxml2中的远程代码执行漏 CVE-2015-3849 2015/08/13 高危 CVE-2016-2426 2016/04/02 中危 信息泄漏 安卓框架中的信息泄漏漏漏 CVE-2015-6764 2015/12/01 高危 CVE-2016-1677 2016/05/25 中危 信息泄漏 Chrome V8 decodeURI 信 CVE-2016-2412 2016/02/26 高危 CVE-2016-1688 2016/05/25 中危 远程攻击 Chrome V8引擎的信息泄漏漏 CVE-2016-2416 2016/02/26 高危 CVE-2016-1688 2016/05/25 中危 校限提升 安卓框架界面中的权限提升 CVE-2016-0826 2016/03/01 高危 CVE-2016-3832 2016/08/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0830 2016/03/01 高危 CVE-2016-3897 2016/08/05 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0847 2016/08/04 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0847 <td></td>	
CVE-2015-7555 2017/05/05 严重 CVE-2017-5053 2017/03/29 高危 远程攻击 pwn2own2017 远程执行源 CVE-2015-1532 2015/01/27 高危 CVE-2016-4658 2017/06/01 高危 远程攻击 libxml2中的远程代码执行源 CVE-2015-3849 2015/08/13 高危 CVE-2016-2426 2016/04/02 中危 信息泄漏 安卓框架中的信息泄漏漏源 CVE-2015-6764 2015/12/01 高危 CVE-2016-1677 2016/05/25 中危 信息泄漏 Chrome V8 decodeURI 信息泄漏 CVE-2016-2412 2016/02/26 高危 CVE-2016-1688 2016/05/25 中危 远程攻击 Chrome V8引擎的信息泄漏 CVE-2016-2416 2016/02/26 高危 CVE-2016-1688 2016/05/25 中危 校限提升 安卓框架界面中的权限提升 CVE-2016-0826 2016/03/01 高危 CVE-2016-3832 2016/08/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0847 2016/03/25 高危 CVE-2016-3897 2016/08/05 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0847 2016/04/02 高危 CVE-2016-3897 2016/09/01 中危 权限提升 <td>: 注制漏洞</td>	: 注制漏洞
CVE-2015-3849 2015/08/13 高危 CVE-2016-2426 2016/04/02 中危 信息泄漏 安卓框架中的信息泄漏漏消 CVE-2015-6764 2015/11/18 高危 CVE-2016-1677 2016/05/25 中危 信息泄漏 Chrome V8 decodeURI 信 CVE-2016-6771 2015/12/01 高危 CVE-2016-1688 2016/05/25 中危 信息泄漏 Chrome V8 decodeURI 信 CVE-2016-2412 2016/02/26 高危 CVE-2016-1688 2016/05/25 中危 远程攻击 Chrome V8 decodeURI 信 CVE-2016-2412 2016/02/26 高危 CVE-2016-1688 2016/05/25 中危 反限提升 安卓框架界面中的权限提升 CVE-2016-2416 2016/02/26 高危 CVE-2016-3760 2016/07/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0826 2016/03/01 高危 CVE-2016-3832 2016/08/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0830 2016/03/01 高危 CVE-2016-3897 2016/09/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0847 2016/04/02 高危 CVE-2016-3921 2016/10/03 中危 权限提升<	
CVE-2015-6764 2015/11/18 高危 CVE-2016-1677 2015/11/18 高危 CVE-2016-1677 2016/05/25 中危 信息泄漏 Chrome V8 decodeURI 信 CVE-2016-2412 2016/02/26 高危 CVE-2016-1688 2016/05/25 中危 远程攻击 Chrome V8 decodeURI 信 CVE-2016-2412 2016/02/26 高危 CVE-2016-1688 2016/05/25 中危 远程攻击 Chrome V8引擎的信息泄漏 CVE-2016-2416 2016/02/26 高危 CVE-2016-2496 2016/06/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0826 2016/03/01 高危 CVE-2016-3832 2016/08/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0830 2016/03/01 高危 CVE-2016-3832 2016/08/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-2497 2016/09/01 中危 有限 VIFI模块中的信息泄漏洞 CVE-2016-3897 2016/09/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-3921 2016/10/03 中危 权限提升 安卓框架界面中的权限提升	最洞
CVE-2015-6771 2015/12/01 高危 CVE-2016-1677 2016/05/25 中危 信息港灣 CHROME V8 decode ONT 信息 CVE-2016-2412 2016/02/26 高危 CVE-2016-1688 2016/05/25 中危 远程攻击 Chrome V8引擎的信息泄液 CVE-2016-2416 2016/02/26 高危 CVE-2016-2496 2016/06/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0826 2016/03/01 高危 CVE-2016-3760 2016/08/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0830 2016/03/01 高危 CVE-2016-3832 2016/08/05 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-2449 2016/03/25 高危 CVE-2016-3897 2016/09/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0847 2016/04/02 高危 CVE-2016-3921 2016/10/03 中危 权限提升 安卓框架界面中的权限提升	
CVE-2016-2412 2016/02/26 高危 CVE-2016-2496 2016/06/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-2416 2016/02/26 高危 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-2016-0826 2016/03/01 高危 CVE-2016-3832 2016/08/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0830 2016/03/01 高危 CVE-2016-2497 2016/08/05 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-2449 2016/03/25 高危 CVE-2016-3897 2016/09/01 中危 付限提升 安卓框架界面中的权限提升 CVE-2016-0847 2016/04/02 高危 CVE-2016-3897 2016/09/01 中危 村限提升 安卓框架界面中的权限提升 CVE-2016-3897 2016/09/01 中危 权限提升 安卓框架界面中的权限提升	息泄漏漏洞
CVE-2016-2416 2016/02/26 高危 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-2016-0826 2016/03/01 高危 CVE-2016-3832 2016/08/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0830 2016/03/01 高危 CVE-2016-2497 2016/08/05 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-2449 2016/03/25 高危 CVE-2016-3897 2016/09/01 中危 有息泄漏 WIFI模块中的信息泄漏漏洞 CVE-2016-0847 2016/04/02 高危 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-2016-0826 2016/03/01 高危 CVE-2016-3832 2016/08/01 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-0830 2016/03/01 高危 CVE-2016-2497 2016/08/05 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-2449 2016/03/25 高危 CVE-2016-3897 2016/09/01 中危 有息泄漏 WIFI模块中的信息泄漏漏 CVE-2016-0847 2016/04/02 高危 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-2016-0830 2016/03/01 高危 CVE-2016-2497 2016/08/05 中危 权限提升 安卓框架界面中的权限提升 CVE-2016-2449 2016/03/25 高危 CVE-2016-3897 2016/09/01 中危 信息泄漏 WIFI模块中的信息泄漏漏浴 CVE-2016-0847 2016/04/02 高危 CVE-2016-3921 2016/10/03 中危 权限提升 安卓框架界面中的权限提升]
CVE-2016-2449 2016/03/25 高危 CVE-2016-3897 2016/09/01 中危 快限提升 安華福采养面中的快限提升 CVE-2016-0847 2016/04/02 高危 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-2016-0847 2016/04/02 高危 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
0 / 5 00 / 6 / 6 / 6 / 6 / 6 / 6 / 6 / 6 / 6	
C\/E 2016 1646 2016/04/15 三台	 漏洞
CVE-2016-2439 2016/05/01 高危 CVE-2017-0495 2017/03/01 中危 信息泄漏 媒体服务中的信息泄漏	
CVE-2016-2476 2016/06/01 高危 CVE-2017-0490 2017/03/01 中危 权限提升 Wi-Fi 权限许可和访问控制	漏洞
CVE-2016-2495 2016/06/01 高危 CVE-2017-0560 2017/04/01 中危 信息泄漏 恢复出厂设置进程中的信息	財露漏洞
CVE-2016-3744 2016/07/01 高危 CVE-2017-0553 2017/04/01 中危 权限提升 libnl 中的提权漏洞	
双手 ラ ク ナク CVE-2017-5056 2017/06/01 中危 远程攻击 Google xml中的UAF漏洞	

严重 高危 中危 远程攻击 权限提升 信息泄漏

手机系统版本分布情况





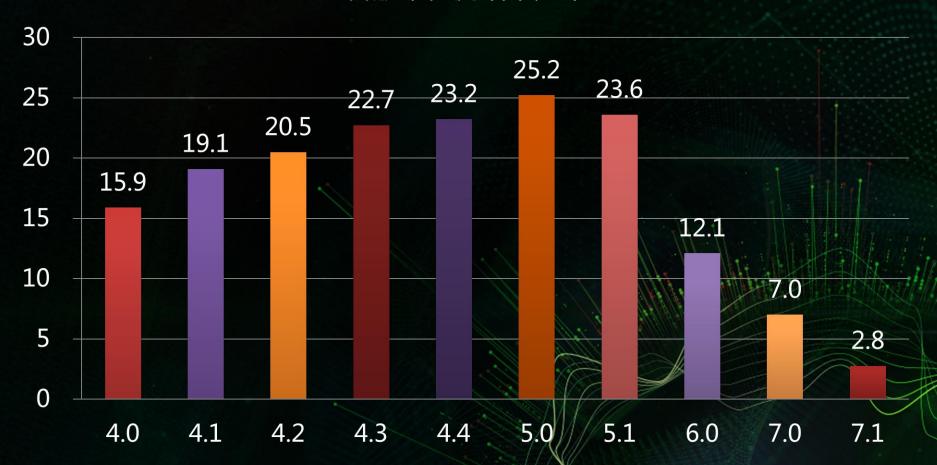


系统各版本平均安全性





各版本检测结果分布

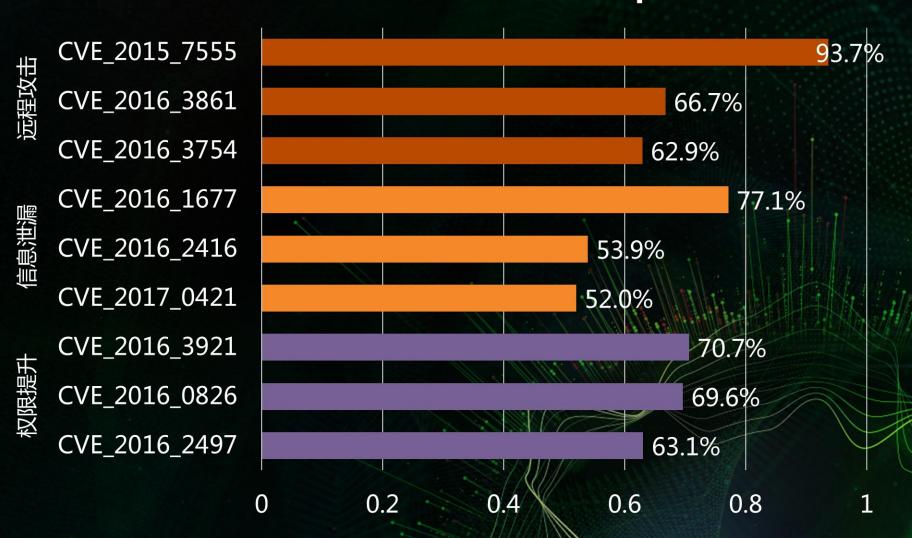


各类型漏洞的"漏洞之王"





不同类型漏洞影响设备比例Top3



不同性别用户安卓手机系统版本分布(部分回访)



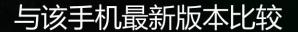


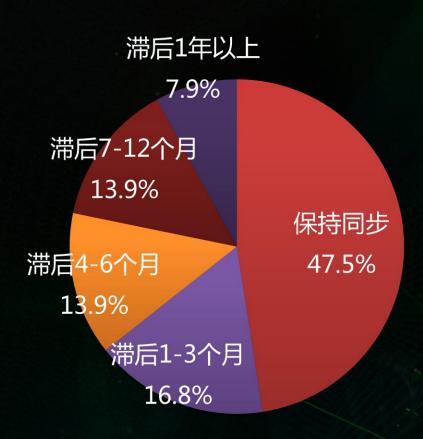


手机系统更新情况

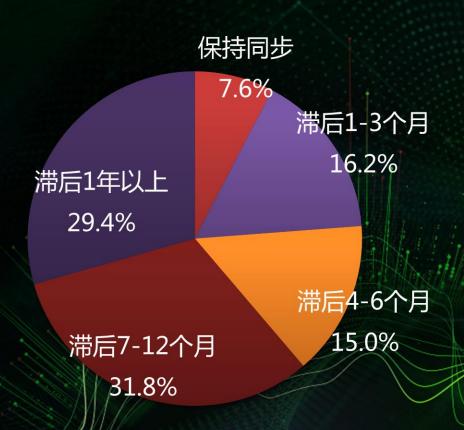








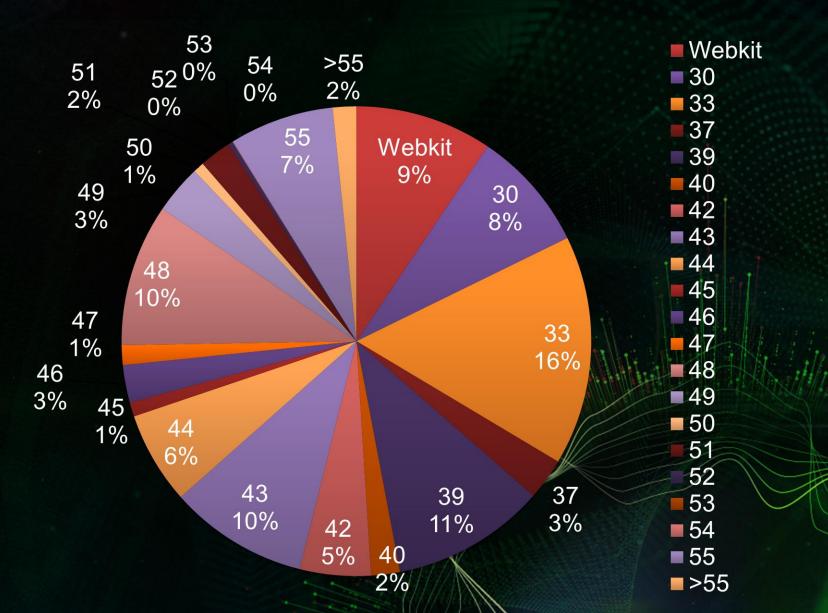
与Google最新版本比较



安卓系统浏览器内核版本分布



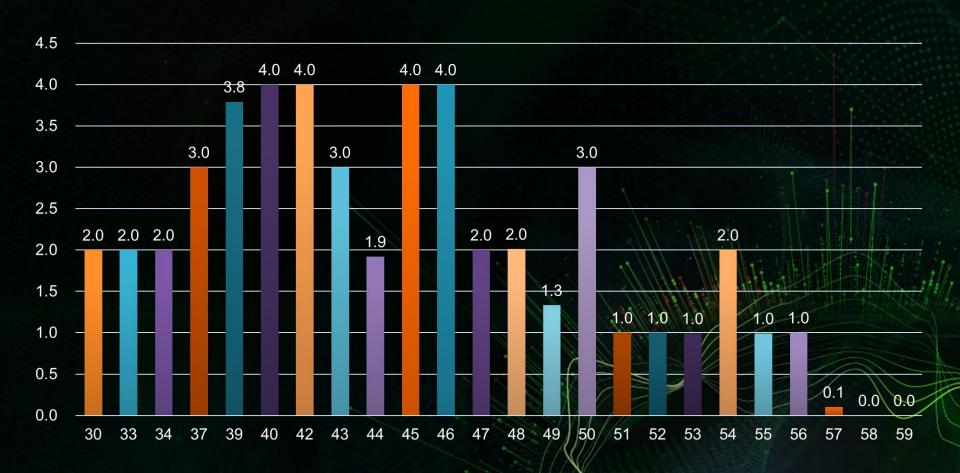




不同版本安卓浏览器平均漏洞个数(共计5)



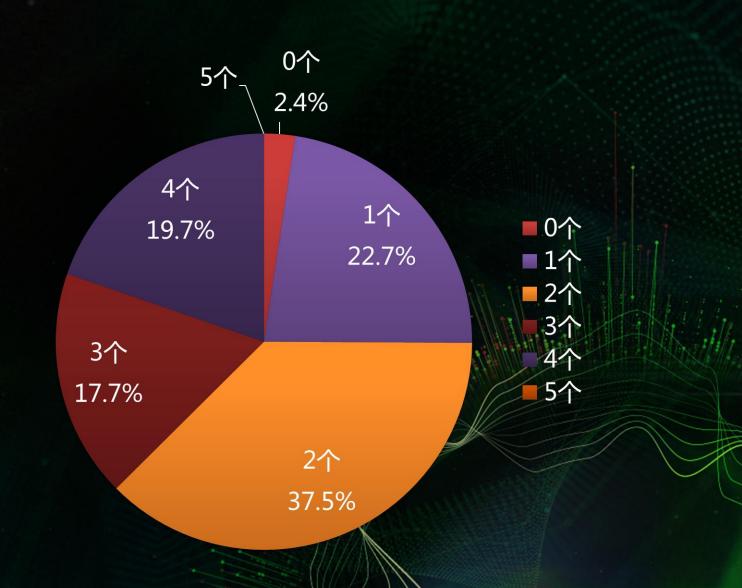




安卓系统浏览器内核漏洞个数比例



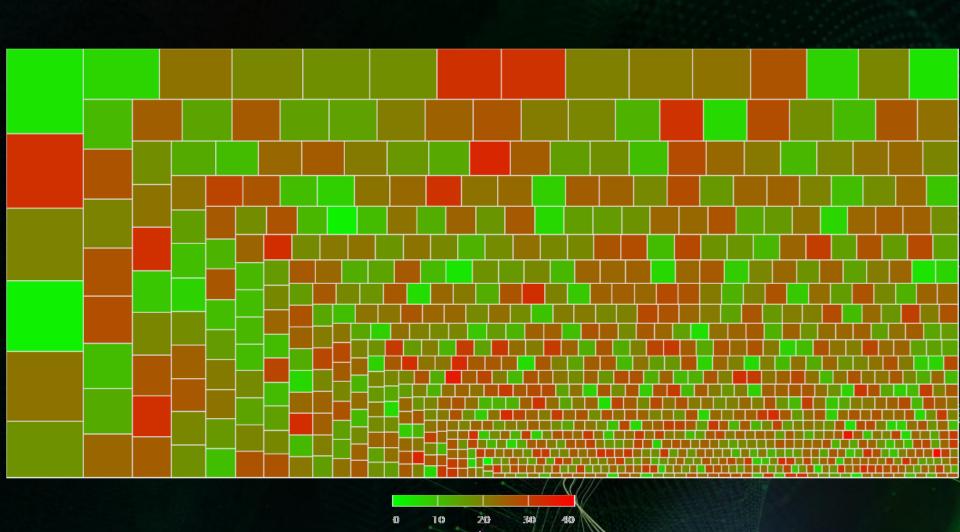




安卓手机系统安全状态(2017.07)





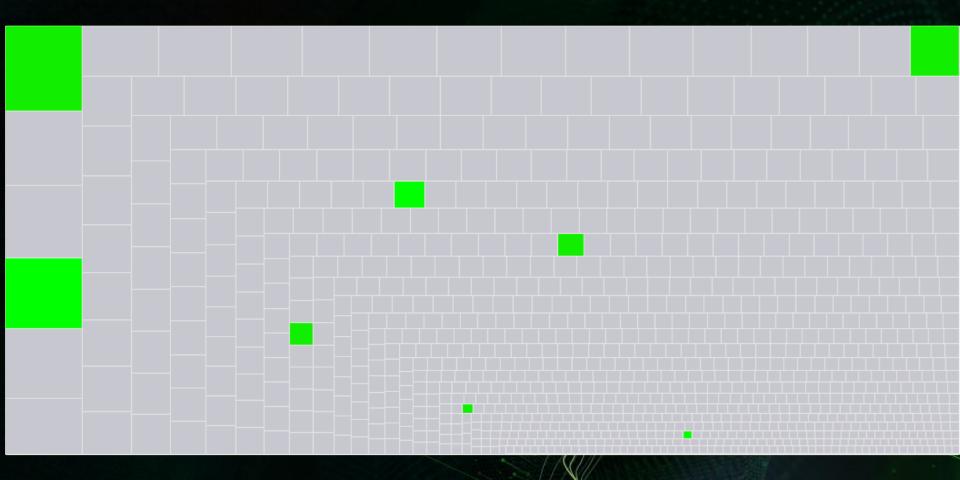


安卓手机系统安全状态(2017.07)





平均漏洞数≤ 5

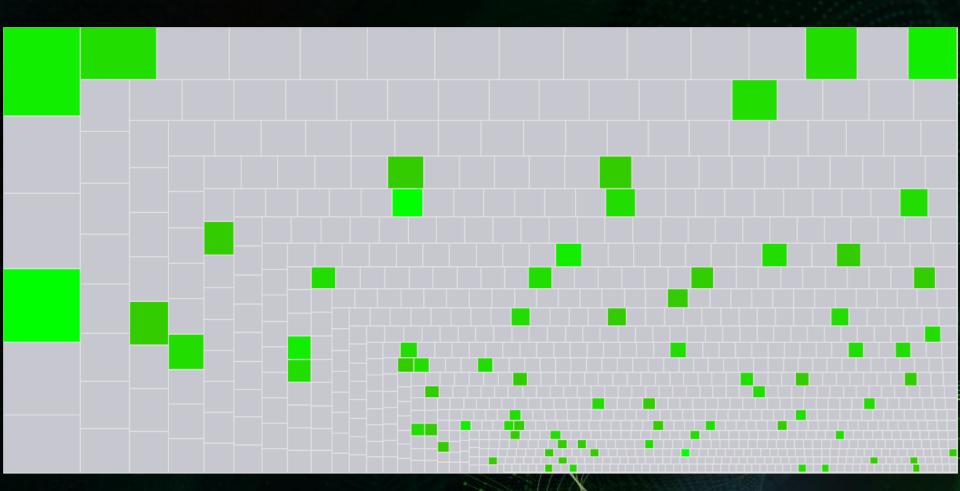


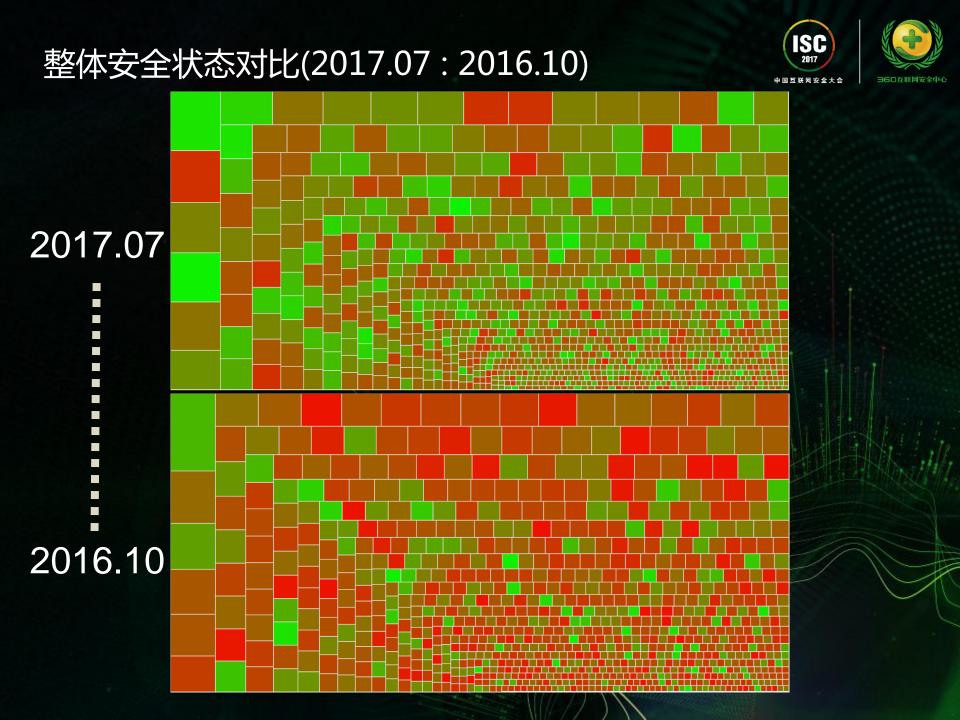
安卓手机系统安全状态(2017.07)





平均漏洞数≤ 10









- 历史N-Day对安卓的影响十分广泛
- 系统更新的滞后性、缺乏统一高效的更新机制 是N-Day影响严重的主要原因
- 浏览器内核漏洞影响广泛,日常浏览网页都可能暴露在风险之中
- 虽然安全性逐渐变好,但是现实中的安卓系统 生态仍然是干疮百孔,系统安全亟待增强

谢谢

