只要1分钟,共享单车的钱就被“骑走”了

十余款单车APP七款有漏洞

只需要一分钟,共享单车的漏洞就被黑客攻陷,用户个人信息被盗取,账户被盗刷。近日,在极客大赛“GeekPwn”年中赛上,小鸣单车、永安行、享骑和百拜四款共享单车APP的漏洞被网名为“tyy”的女程序员轻松破解。tyy直接获取了用户的个人资料,并现场远程连线,演示利用他人账户,实现开锁、骑行的过程。而被攻击的单车企业则表示,对存在的漏洞正在进行修复。

在极客大赛上,黑客小谭利用共享单车APP漏洞,1分钟内就获取了个人信息。

后台被他人登录 账户被盗刷

由国内顶尖信息安全团队碁震(KEEN)发起并主办的GeekPwn(极棒),与Pwn2Own、Defcon并称为世界三大黑客赛事,至今已举办四届。今年的GeekPwn大赛吸引了数十位国内外顶尖的白帽黑客同场炫技,包含智能锁、平衡车、主流手机、路由器等都成为选手的目标。

毕业于浙大计算机专业的“tyy”是此次参赛的唯一女黑客。记者联系到网名为“tyy”的女黑客小谭,她回忆了当时的比赛现场。“评委老师在现场用自己的手机使用共享单车APP,我在电脑上操作,利用APP的程序漏洞,攻击评委老师的应用后台,我就拿到了他的账户余额、骑行记录。”

另外,身在香港参加比赛的小谭还在现场远程连线在上海的朋友,演示了攻击APP账户后骑行消费的过程。“我把自己通过漏洞掌握的信息,同步给上海的朋友,上海的朋友演示扫码骑车,并攻击了评委的APP账户,评委刷新后,就发现多了一条骑行消费的行程。”小谭说。

小谭如今在上海当一名程序员。对于如何发现共享单车的漏洞,小谭称:“现在共享单车很火,我自己也在用,而且我会写代码,我就想如果这APP是我做,别人会怎么攻击它呢?我就把市面上的APP差不多都尝试了一下。”

小谭在大概一个月时间里,尝试攻击了十几款共享单车APP,最终她发现其中7款有问题,比赛中,她选择了小鸣单车、永安行、享骑和百拜这四款。“剩下的三款不便于在大赛上演示,是因为有的车辆很少,并没有很完整的攻击链,所以没有拿到比赛上,但以我的代码经验来看,是有问题的。”

小谭回忆,她最早看出问题的是摩拜单车,“我是某个周五早上看出来有漏洞,摩拜修复得很快,他们在当天晚上就修复了,我再试验的时候,他们的漏洞已经修好了。”

1分钟就能攻破 个人信息也被“共享”

小谭说,她通过篡改输入参数,进而直接访问、控制他人账号。获取用户的个人账户信息后,登录自己的账户扫码骑车,扣的却是别人账户的余额。她认为,这些漏洞的危害性不仅在于用户损失金钱,更重要的是隐私泄露。

对于攻破共享单车账户的技术难度有多大的问题,小谭说,“这四款APP攻击漏洞难度并不一样,有些容易,有些非常简单。”

究竟利用这个漏洞完成攻击会有多快?“一分钟并不夸张,甚至更短”。

小谭说,“你在使用APP的过程中,我利用程序漏洞,抓取到需要的内容,可以很快获取你的个人信息,而且有几款APP即便退出登录、改密码也是没有用的。当时比赛是限时30分钟,我演示四个APP,没有详细算时间,我从拿到原始信息开始,并且逐个APP展示,中间也有一些重连服务器的耗时情况,比赛完成后,我并没有超时。”

“一些程序员可能不会想到这些问题,但如果有一些反向思维,有保护用户个人信息的意识,对信息安全有了解,可能这四款APP就避免了类似的漏洞。希望更多的人关注信息安全。”小谭说。

17日,记者联系到极客大赛GeekPwn主办方,对于如何确保小谭及其他参赛选手技术操作的真实性,对方作了回应。

“为了保证真实性,我们的比赛都是现场进行的,业界的评委在台上进行观看,通过选手的操作(电脑上的攻击代码)等专业标准进行评判,赛后,也会马上让获奖选手进入漏洞披露室披露技术细节。”主办方工作人员说。

漏洞已提交厂商 三家企业正在修复

业内人士认为,这暴露出共享单车云端的漏洞技术含量很低。近年我国“风口”互联网行业发展速度远远大于技术发展速度,技术发展速度又远远大于安全能力发展的速度。可能有些行业实践超过美国十年,但安全能力却落后十年。

有网友看到这则报道后担心,既然这个女黑客已经破解了这四款单车的漏洞,那么不就相当于将这些漏洞告知所有人,让一些不法之徒利用吗?

极客大赛的主办方对此质疑回应称,“极棒赛后会将漏洞细节义务提交给厂商,协助其修复漏洞,从而消除安全隐患。而选手提交给极棒漏洞,极棒给予选手奖金,鼓励其创新思维和技术。”

随后,记者分别致电永安行、小鸣单车、享骑和百拜厂商,了解漏洞修复进程。

小鸣单车市场总监张恒也在第一时间给予回应:“确实收到了大赛提交的漏洞,现在这些具体的漏洞我们都已经修复好了,这样的比赛还是很友好的,及时发现问题,及时反馈给厂商。”百拜单车CMO张宝俊表示:“已经收到极客大赛反馈的漏洞,现在已经解决了部分,其他部分也正在紧急处理。”

享骑出行回复称,已收到主办方发送的程序漏洞的邮件,正在加紧修复。截至记者发稿时,永安行方面还未回复。 **据法晚、广州日报等**

住房租售首部法规征意见

房租多押一付三 按月支付或成主流

本报讯 5月19日,我国首部专门针对住房租赁和销售的法规——《住房租赁和销售管理条例》(征求意见稿)开始向社会公开征求意见。立法的目的在于规范住房租赁和销售行为,保护当事人合法权益,保障交易安全。

据统计,我国约有1.6亿人在城镇租房居住,主要是外来务工人员、新就业大学生等。意见稿中,对保护承租人权益着墨颇多,在租金、租期、承租人居住权利保障等方面作了规定。

为减轻承租人集中支付租金的压力,征求意见稿规定,除当事人另有约定外,承租人应当按月支付租金。对住房租赁合同中未约定租金调整次数和幅度的,出租人不得单方面提高租金。征求意见稿鼓励出租人与承租人签订长期住房租赁合同,对于当事人签订三年以上住房租赁合同的,规定直辖市、市、县人民政府要给予相关政策支持。对于住房租赁企业出租自有住房的,除承租人另有要求外,租赁期限不得低于三年。针对二房东转租他人住房违规经营等市场乱象,征求意见稿规定,转租住房应当征得出租人的书面同意,对于自然人转租住房达到一定规模的,应当依法办理工商登记。

征求意见稿强化了对房地产开发企业销售住房行为的监管。

房地产开发企业在取得预售许可证后,应当在十日内在房产管理部门网站和销售现场一次性公开全部准售住房及每套住房价格,并对外销售。对于房地产开发企业现售住房的,实行现售备案制度。房地产开发企业存在发布虚假广告、哄抬房价、捂盘惜售、价外加价、一房多售、捆绑销售等12项禁止性行为的,可依法处以暂停网上签约权限、没收违法所得、罚款、吊销资质证书等处罚措施。

为加强房地产中介行业管理,规范服务行为,征求意见稿也作了具体规定。

中介机构和从业人员不得捏造散布不实价格信息、炒卖房号、发布虚假房源信息、捆绑收费、赚取差价、违规提供购房融资、为当事人规避税费提供便利等11项禁止性行为。经纪机构和从业人员违反上述规定的,征求意见稿规定了给予暂停合同网上签约权限、没收违法所得、罚款等较为严厉的处罚措施。

此外,公租房等政策性住房租赁和销售,以及旅馆类住宿服务,不适用该条例的规定。 **据人民日报**