

亚洲诚信助力看雪安全开发者峰会

转载

[weixin_34357887](#) 于 2017-11-20 16:46:00 发布 51 收藏

文章标签: [网络](#) [嵌入式](#) [python](#)

原文链接: <https://my.oschina.net/u/3501961/blog/1576219>

版权

[2019独角兽企业重金招聘Python工程师标准>>>](#) HOT



11月的北京，寒风初上。冷冽的空气中，透露着北京这座古都的庄严。2017看雪安全开发者峰会就在北京悠唐皇冠假日酒店举行。

来自全国各地的开发人员、网络安全爱好者及相应领域顶尖专家，都在2017看雪安全开发者峰会汇聚一堂，只为这场“安全与开发”的技术盛宴。



从早上8点开始，北京悠唐皇冠假日酒店，便有络绎不绝的听众赶来签到，场面火爆。会场爆满，会场后面都挤满了站着的人。

本次会议的主持人为北京启明星辰ADLab副总监、集团首席技术组成员侯浩俊，他幽默风趣的主持风格，带起了台下一阵又一阵的欢笑。

来自中国信息安全测评中心总工程师王军在致辞中提到：“带来网络安全根本性的问题有几个：1，系统复杂性。2，系统存在漏洞。3，还存在着对手的威胁。在这几个问题当中，如何解决需要从问题的根源，也就是从开发阶段，从产品以及系统的生产阶段解决，这是我们解决的根本途径之一。因此，看雪论坛组织安全者开发的讨论是非常有意义的。”

看雪论坛二进制漏洞版块版主——仙果带来峰会的第一个议题《Flash之殇-漏洞之王Flash Player的末路》。针对Flash Player为题，他为大家展现了Flash Player的漏洞利用史，并讲解了Flash漏洞利用技术和攻防对抗技巧。

核心数据是怎么被黑客泄露的呢？黑客又是如何进入后台系统的？有偿删帖是如何实现的？小学生又是如何1分钱购买商品的？中国婚博会高级PHP工程师汤青松在看雪峰会上用形象生动的方式给予了答案，以及应对方案。

威胁猎人的产品总监彭巍，解析国内业务安全发展过程，帮助甲方研发梳理业务安全对抗思路并对当前主要的一些风险场景做具体说明。并面向行业痛点发布两个开源项目，帮助行业大量的中小企业实现业务风控的快速落地。

陆麟，Windows系统内核专家，长期研究系统内核。在此次看雪峰会上分享了他在Windows的Linux中研发出来的一些成果，即可以直接在Windows下直接执行的Linux。以及一个windows 10的0day漏洞，引发大家的关注。

启明星辰ADLab西南团队负责人王东，首先用智能门锁为例，对WIFI和BLE两种组网类型的智能设备进行安全漏洞分析，并指出日常生活中智能应用的典型安全漏洞。最后分享我们在工业控制系统方面的安全研究经验。

在本次峰会上，陈愉鑫揭露了多个真实案例的技术细节、开发流程、运营流程，描述了一条以刷单、倒卖、刷榜、引流、推广为主的灰色产业链。并提出一些防护建议，协议安全需要从体系上进行加强。

腾讯反病毒实验室安全研究员在此次峰会上分享了包括IoT root设备的技术手段、获得root权限后引发的潜在安全威胁，和缓解安全威胁的一些方法。还分享了已提交CNNVD的IoT设备root漏洞。

绿盟科技应急响应中心Web研究员邓永凯将对开发者在开发编码时最容易产生漏洞以及意料之外的漏洞进行分析，阐述其原因以及应该注意的地方。通过没有防御到防御绕过、错误的防御姿势、错误的使用方法、错误的修复方法、系统及语言自身特性、设计缺陷、二次漏洞、程序员的惰性导致的漏洞等方面进行了实例讲解。

本议题，腾讯游戏安全高级工程师胡和君以FPS类型游戏的自瞄外挂功能的对抗为例，通过对自瞄外挂实现原理解析，阐述了如何使用定制化的技术思想，达到对外挂作弊功能的持续压制。另外议题中还谈及游戏漏洞挖掘的核心思路和方法技巧，游戏开发者自身提升游戏安全性的技术手段，安全防守方定制化方案分析、开发、实现的方法和技巧等内容。

在这次演讲中，绿盟科技网络安全攻防实验室安全研究员廖新喜，阐述了Java JSON库的反序列化特性导致的RCE。此外还公布了一些未公开的反序列化的payload（以Fastjson举例说明）并会对这些payload进行了分类解读。最后从开发、维的角度来提出了防御方案。

看雪论坛iOS版主roysue针对应用层的攻击频次连年增长，攻击方式更加多元的现象，提出了相应的策略。

阿里安全IoT安全研究团队Leader，谢君系统的介绍了某品牌无人机的架构体系、功能模块、传感器等，包括各个组件的攻击面、安全防护体系、软硬件反调技术及其绕过方法，并深度解读无线宽带通信等。此外在峰会现场谢君还介绍一个不需要通过软件漏洞就能Root无人机的方法，并演示了如何远程劫持一台无人机，引发现场热烈的掌声。



在大家热烈的掌声中，2017看雪安全开发者峰会落下帷幕。但这不是结束，而是起点。看雪将不忘初心，继续为大家营造一个更好良好的技术交流平台，同时携手亚洲诚信继续带领大家在安全领域继续砥砺前行，为互联网安全发展做出贡献。

以开发会安全，以安全辅未来!

转载于:<https://my.oschina.net/u/3501961/blog/1576219>