安全小课堂第四十六期【Redis 未授权访问漏洞】

京东安全应急响应中心 2017-02-24

亲，戳上面的**蓝字**关注我们哦！

Redis 未授权访问漏洞

期数：第四十六期

讲师：valo

讲师简介：长亭科技首席安全官，多项国内重要网络安全对抗赛的冠军。曾任国内第一家安全众测平台技术负责人，参与了不同领域上百家大型企业的网络安全测试修复工作。

ISC 安全训练营讲师，Qcon、Wot、京东安全峰会等重要会议讲师；

JSRC核心白帽子、TSRC核心白帽子。

专注于应用安全、渗透测试、安全架构、漏洞挖掘等领域。

Redis是什么？Valo师傅能简述一下Redis未授权访问漏洞吗？

京安小妹

Redis是大家常说的非关系型数据库中的一种，是一个开源的使用ANSI C语言编写、支持网络、可基于内存亦可持久化的日志型、Key-Value数据库，并提供多种语言的API。

Redis与memcached一样，为了保证效率，数据都是缓存在内存中。但Redis会周期性的把更新的数据写入磁盘或者把修改操作写入追加的记录文件，并且在此基础上实现了master-slave(主从)同步。

Redis未授权访问漏洞是指入侵者访问到没有权限限制的Redis时可获取数据库里的所有内容，造成信息泄露等危害。

讲师：Valo

Redis未授权漏洞如何形成的呢?

京安小妹

Redis默认会开放6379端口，如果在配置服务时，端口开放在了0.0.0.0上，而防火墙也没有做防护，就会导致其他机器可以访问该端口，而如果没有设置连接密码，就造成了未授权访问漏洞。

讲师：Valo

能描述下Redis未授权漏洞的危害吗?

京安小妹

Redis未授权访问的危害分两个层面，一个是数据层面一个是系统层面。

大家都知道Redis中存储的是大量的数据，如果被黑客恶意访问到，即可对其中的数据进行增删改查，危害巨大。

至于系统层面的危害，需要跟Redis启动的权限结合。简而言之，Redis具有写文件的功能，对应其运行权限，可以写不同的文件，如web文件、crontab文件、ssh的authorized_keys等，进而造成成不同的危害。

讲师：Valo

如何检测Redis未授权漏洞呢?

京安小妹

找的话，网管的话自己有什么自己知道，想想符不符合上面说的漏洞特征就行。
黑客的话，爱怎么找怎么找吧。

讲师：Valo

白帽子观点

扫描所有开了6379的IP

作为企业如何修复Redis未授权访问漏洞呢?

京安小妹

根据上面说的，问题的成因和风险点已经很清楚了，那么就可以做对应的修复和防护。首先要给Redis的访问加上密码，然后对网络进行限制，如果是本机使用，可以将端口开放在127.0.0.1，如果必须外部访问，那么设置防火墙白名单。最后把Redis的启动权限降至nobody就可以了。

讲师：Valo

Valo师傅还有什么需要补充的吗?

京安小妹

测试Redis的时候，**千万不要用带有flushall的exp啊**！因为会清空数据库。

讲师：Valo

白帽子提问

不能使用扫描器，或者许多漏洞的poc都无法批量去验证查询?
手动的话如何去高效和全面的去挖掘漏洞呢（担心有些面覆盖不全）
是否需要我们平常把每个漏洞都需要梳理和熟悉记录成笔记?
然后测试的时候直接参照笔记来做测试呢?（因为有些测试还禁止使用公网搜索信息）

这个问题是逼我做广告啊，我们长亭科技的安服团队在测试过程中就不允许使用扫描器，纯手工测试，天然无公害。当然这不是为了装逼，是怕扫描器影响客户业务。 这里指的扫描器是指web扫描器，收集自域名啊什么的当然还是要自动化一下。

至于web扫描器节省人力的地方就是爬虫，然后fuzz各种漏洞，如果要人去做，如果做到面全，就需要人工收集到每一个点每一个参数，对于找到的点，不一定要遍历所有漏洞类型，要根据业务和经验判断这个点可能存在的问题来提高效率。

当然，人工还有比扫描器好的地方，可以发现逻辑漏洞，可以发现注释掉的或者隐藏在js中的漏洞等。

关于笔记的话，我也是有一个自己的文档库，但是这里面大多是一些cms公开的poc、提权exp等，sql注入语法、域渗透命令之类的属于基础知识，必须死记到脑子里。

讲师：Valo

白帽子提问 **redis有没有日志，记录那些来源IP连了redis？**

ip来源记录的话，这个我也不清楚，不过讲道理应该会有记录的。

讲师：Valo

白帽子提问 **配合ssh_key时会对数据库的使用造成影响吗?**

配合ssh_key不会对数据库的使用造成影响，倒是可能会利用不成功，如果redis本身存在了大量数据，又不能flushall，写入sshkey后可能导致ssh卡死连不上。

讲师：Valo

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，回复“安全小课堂”或者点击阅读原文进行查看。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心

阅读原文