# 0001

漏洞名称：Fastjson 1.2.24反序列化漏洞分析

漏洞时间：2017

CVE编号：无

影响平台：windows、linux

影响范围：Fastjson1.2.2≤1.2.24

介绍：fastjson接受的JSON可以通过@type字段来指定该JSON应当还原成何种类型的对象，在反序列化的时候方便操作。因为可以还原成任何类型的对象，因此造成了REC漏洞。

EXP：Fastjson 1.2.24

# 0002

漏洞名称：Fastjson1.2.60拒绝服务漏洞

漏洞时间：2019-9-5

CVE编号：暂无

影响平台：windows、linux

影响范围：Fastjson ＜ 1.2.60

介绍：漏洞的关键点在com.alibaba.fastjson.parser.JSONLexerBase#scanString中，当传入json字符串时，fastjson会按位获取json字符串，当识别到字符串为x为开头时，会默认获取后两位字符，并将后两位字符与x拼接将其变成完整的十六进制字符来处理，而当json字符串是以x结尾时，由于fastjson并未对其进行校验，将导致其继续尝试获取后两位的字符。也就是说会直接获取到u001A也就是EOF，当fastjson再次向后进行解析时，会不断重复获取EOF，并将其写到内存中，直到触发oom错误。

POC: Fastjson1.2.60拒绝服务(非pocsuit插件)

# 0003

漏洞名称：Fastjson1.2.48反序列化漏洞补丁绕过

漏洞时间：2019-7-11

CVE编号：暂无

影响平台;windows、linux

影响范围：Fastjson 1.2.48以下的版本（不包括1.2.48）

介绍：Fastjson在1.2.48版本以下，无需Autotype开启，攻击者即可通过精心构造的请求包在使用Fastjson的服务器上进行远程代码执行。

EXP: fastjson = 1.2.47 反序列化漏洞

# 0004

漏洞名称：