JFasterxml Jackson-databind 远程代码执行漏洞(CVE-2020-35728)
安全通告

2020 年 12 月 28 日

目录

一、 漏洞概要 3
二、 漏洞分析 4
三、 影响范围 5
四、 解决方案 6

一、 漏洞概要

漏洞名称	Fasterxml Jackson-databind 远程代码执行漏洞(CVE-2020-35728)
威胁等级	高危
影响范围	2.0.0 <= Fasterxml <= 2.9.10.8
安全版本	Fasterxml >= 2.10.x
漏洞类型	远程执行代码
利用难度	简单

二、 漏洞分析

2.1 组件介绍

Jackson 是当前用的比较广泛的，用来序列化和反序列化 json 的 Java 的开源框架。Jackson 社区相对比较活跃，更新速度也比较快，从 Github 中的统计来看，Jackson 是最流行的 json 解析器之一。SpringMVC 的默认 json 解析器便是 Jackson。Jackson 优点很多。Jackson 所依赖的 jar 包较少，简单易用。与其他 Java 的 json 的框架 Gson 等相比，Jackson 解析大的 json 文件速度比较快；Jackson 运行时占用内存比较低，性能比较好；Jackson 有灵活的 API，可以很容易进行扩展和定制。

Jackson 的 1.x 版本的包名是 org.codehaus.jackson ，当升级到 2.x 版本时，包名变为 com.fasterxml.jackson。

2.2 漏洞描述

2020 年 12 月 27 日， jackson-databind 官方发布安全通告， 披露 jackson-databind < 2.9.10.8 存在反序列化远程代码执行漏洞，利用漏洞可导致远程执行服务器命令。该漏洞是由 JNDI 注入导致远程代码执行，Jackson-databind 2.0.0-2.9.10.8 版本中缺少 com.oracle.wls.shaded.org.apache.xalan.lib.sql.JNDIConnectionPool 黑名单类，攻击者可以利用上述缺陷，绕过限制，实现 JNDI 注入，最终在受害主机上执行任意代码。

三、 影响范围

3.1. 受影响版本

2.0.0 <= Fasterxml <= 2.9.10.8

3.2. 安全版本

Fasterxml >= 2.10.x

四、 解决方案

4.1、官方解决方案

官方已发布新版本修复此漏洞。

下载链接：https://github.com/FasterXML/jackson-databind/releases