ONEStor是否涉及Apache log4j 1.0相关漏洞

程鑫 2022-01-21 发表

漏洞相关信息

漏洞编号： CVE-2022-23302、CVE-2022-23305、CVE-2022-23307
漏洞名称： Apache log4j 1.0相关漏洞
产品型号及版本： ONEStor产品

漏洞描述

Apache log4j JMSSink反序列化代码执行漏洞（CVE-2022-23302）：当攻击者具有修改Log4j配置的权限或配置引用了攻击者有权访问的LDAP服务时，Log4j1.x所有版本中的JMSSink 都容易受到不可信数据的反序列化。攻击者可以提供一个TopicConnectionFactoryBindingName配置，利用JMSSink执行JNDI请求，从而以与CVE-2021-4104类似的方式远程执行代码。Log4j默认配置时不受此漏洞影响。

Apache log4j JDBCAppender SQL注入漏洞（CVE-2022-23305）：由于Log4j 1.2.x中的JDBCAppender接受SQL语句作为配置参数，PatternLayout的消息转换器未对其中输入的值进行过滤。攻击者可通过构造特殊的字符串到记录应用程序输入的内容中来操纵SQL，从而实现非法的SQL查询。Log4j默认配置时不受此漏洞影响。

Apache log4j Chainsaw反序列化代码执行漏洞（CVE-2022-23307）：Log4j 1.2.x中的日志查看器Chainsaw中存在反序列化问题，可能造成任意代码执行，该漏洞此前被命名为CVE-2020-9493，官方已发布Apache Chainsaw 2.1.0版本进行修复。Log4j默认情况下未配置Chainsaw使用。Chainsaw v2是由Log4j开发社区成员编写的与Log4j配套的应用程序，是一个基于GUI的日志查看器，可以读取Log4j的XMLLayout格式的日志文件。

受影响版本 • Apache Log4j 1.x • Apache Chainsaw < 2.1.0

漏洞解决方案

ONEStor不涉及

未使用漏洞描述中JMSSink 、JDBCAppender 、Chainsaw相关配置