ADWAN5.0承载网方案相关产品不涉及Apache Log4j多个安全漏洞（非Apache Log4j2）

ADWAN解决方案 田毓磊 2022-01-26 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 JMSSink反序列化代码执行漏洞、Apache log4j JDBCAppender SQL注入漏洞、Apache log4j Chainsaw反序列化代码执行漏洞
产品型号及版本： SNA Center E1211、SeerEngine-WAN E6105H12、SeerAnalyzer E2101P10、License Server E1153

漏洞描述

（1）Apache log4j JMSSink反序列化代码执行漏洞
CVE: CVE-2022-23302
组件: JMSSink
漏洞类型: 代码执行
漏洞等级：高危
影响: 服务器接管
简述: 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，所有 Log4j 1.x 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，使JMSSink执行JNDI请求，从而以与CVE-2021-4104类似的方式远程执行代码。
注意：此漏洞仅在专门配置为使用 JMSSink时影响 Log4j 1.x。Log4j默认配置时不受此漏洞影响。

（2）Apache log4j JDBCAppender SQL注入漏洞
CVE: CVE-2022-23305
组件: JDBCAppender
漏洞类型: SQL注入
漏洞等级：高危
影响: 数据泄漏,命令执行
简述: 由于Log4j 1.2.x中的JDBCAppender接受SQL语句作为配置参数，而PatternLayout的消息转换器未对其中输入的值进行过滤，就导致了SQL注入漏洞。该漏洞允许攻击者在记录应用程序输入的内容或标题中插入恶意构造的字符串来操纵SQL，从而实现非法的SQL查询。
注意：此漏洞仅在专门配置为使用 JDBCAppender时才会影响 Log4j 1.x， Log4j默认配置时不受此漏洞影响。

（3） Apache log4j Chainsaw反序列化代码执行漏洞
CVE: CVE-2022-23307
组件: Chainsaw
漏洞类型: 代码执行
漏洞等级：严重
影响: 服务器接管
简述: 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。该漏洞存在于Log4j 1.2.x中的日志查看器Chainsaw中，是一个反序列化漏洞，可造成任意代码执行。该漏洞此前被命名为CVE-2020-9493。建议用户升级到Apache Chainsaw 2.1.0版本和Log4j 2 以进行安全修复（Apache 已于 2015 年停止维护 Log4j 1.x）。
注：此漏洞仅在专门配置为使用Chainsaw时才会影响 Log4j 1.x， Log4j默认配置时不受此漏洞影响。

漏洞解决方案

SNA Center、SeerEngine-WAN、SeerAnalyzer、License Server产品不涉及Apache log4j JMSSink反序列化代码执行漏洞、Apache log4j JDBCAppender SQL注入漏洞、Apache log4j Chainsaw反序列化代码执行漏洞。