iMC v7及U-Center1.0产品关于Apache log4j2漏洞

PLAT Ucenter **李大维** 2021-12-14 发表

漏洞相关信息

漏洞编号： CVE-2021-44228

漏洞名称： Apache Log4j2 远程代码执行漏洞

产品型号及版本： PLAT E0706至 PLAT E0706P06版本涉及；EIA_E0620-E0622区间版本；U-Center_E0707L06-E0709H05区间版本

漏洞描述

Apache Log4j2 是一款开源的 Java 日志记录工具，大量的业务框架都使用了该组件。此次漏洞是用于 Log4j2 提供的 lookup 功能造成的，该功能允许开发者通过一些协议去读取相应环境中的配置。但在实现的过程中，并未对输入进行严格的判断，从而造成漏洞的发生。

此次受影响版本如下：

Log4j版本

是否受影响

2.x<=2.14.1

漏洞解决方案

PLAT E0706之前版本使用log4j，版本为1.2.17

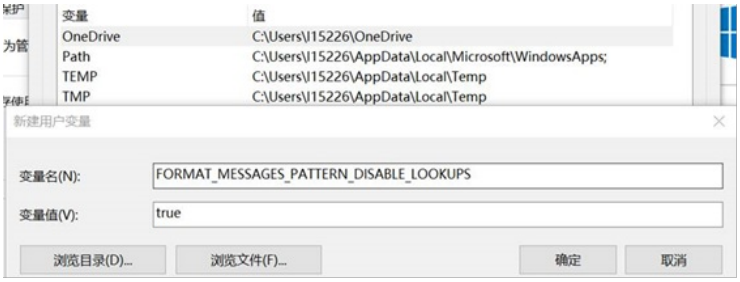
PLAT E0706至E0706P06版本使用log4j2，版本为2.14.0

漏洞修复方法：

windows环境下修复方法二选一即可，若涉及同步修复UCenter组件漏洞，只能选择方法一

方法一：需重启操作系统

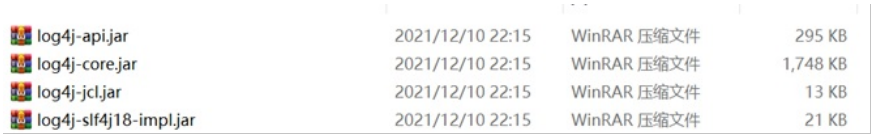
若可以重启操作系统，新增环境变量FORMA_MESSAGES_PATTERN_DISABLE_LOOKUPS=true后重启操作系统后启动iMC生效



方法二：无需重启操作系统：

1、请将四个jar包备份后将附件jar包替换至如下安装目录：

\iMC\client\repository\log4j\jars



2、增加环境变量FORMAT_MESSAGES_PATTERN_DISABLE_LOOKUPS=true

3、重启IMC服务后部署监控代理右键启动jserver进程（不要用startup脚本启动）

Linux环境下：

在系统环境变量 中增加一行FORMAT_MESSAGES_PATTERN_DISABLE_LOOKUPS = true

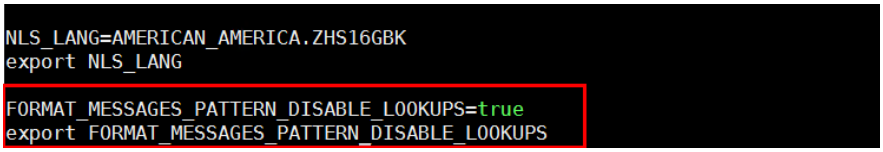
操作如下：

1、修改环境变量文件，vi /etc/profile

2、在文件中增加环境变量信息

FORMAT_MESSAGES_PATTERN_DISABLE_LOOKUPS=true

export FORMAT_MESSAGES_PATTERN_DISABLE_LOOKUPS



增加后esc退出编辑模式，通过:wq保存文件

4、修改配置文件后需环境变量生效，生效方式分为两种：

a）重启操作系统

b) source /etc/profile生效，之后重启iMC的dms服务（iMC/deploy目录下执行./dms.sh stop后再./dms.sh start），再重新打开部署监控代理即可

附件下载：替换.zip