U-Center2.0产品关于Apache log4j2漏洞

U-Center 2.0 汤祺 2021-12-15 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_2.0_E0613及PLAT_2.0_E0706以前版本都涉及，UC组件及EIA/EAD组件不涉及

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

修复版本：可通过升级PLAT_2.0版本至E0613及以上或者E0706及以上版本修复，组件版本需查看版本说明书中平台版本的适配关系确认是否需要同步升级

临时规避方案如下：

1. elasticsearch的修改如下：

a） 通过ssh登陆统一数字底盘后台任意节点；

b） 获取涉及此漏洞的资源名称：

kubectl get statefulset -A | grep elasticsearch

如下图所示，通过命令查询到涉及漏洞elasticsearch组件有3个，需对3个资源分别进行修复

```
[root@matrix01 Packages]# kubectl get statefulset -A | grep elasticsearch
service-software   elasticsearch-node-1   1/1     46d
service-software   elasticsearch-node-2   1/1     46d
service-software   elasticsearch-node-3   1/1     46d
```

c） 编辑资源配置，增加环境变量：

kubectl edit statefulset [资源名称] -n service-software

在env段加入如下内容：

- name: FORMAT_MESSAGES_PATTERN_DISABLE_LOOKUPS
  value: “true”
- name: JAVA_TOOL_OPTIONS
  value: “-Dlog4j2.formatMsgNoLookups=true”

```
   containers:
   - env:
     - name: FORMAT_MESSAGES_PATTERN_DISABLE_LOOKUPS
       value: “true”
     - name: JAVA_TOOL_OPTIONS
       value: “-Dlog4j2.formatMsgNoLookups=true”
     - name: NONROOT_PROC_LIMIT
       value: "8192"
     - name: CLUSTER_NAME
       value: elasticsearch-cluster
```

d） 按下Esc键，输入:wq保存，相关服务会自动重启，第二步命令返回的3个资源配置都需进行修改

2. logstash操作如下：

a） 通过ssh登陆统一数字底盘后台全部节点,创建目录/opt/matrix/app/data/base-service/log-center/logstash，将附件解压后的脚本rm_jndi.sh拷贝到目录下

b） 通过ssh登陆统一数字底盘后台任意节点；

c） 编辑资源配置

kubectl edit deployment logstash -n service-software

在path.settings下面增加command启动命令：

--path.settings=/usr/share/logstash/config

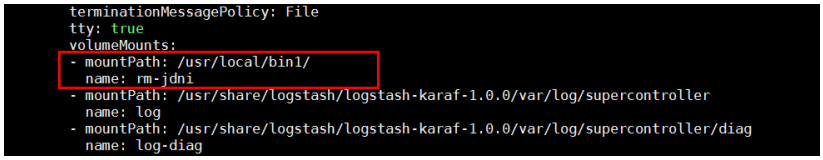
command:

- /bin/sh
- /usr/local/bin1/rm_jndi.sh

```
    - args:
      - --config.reload.automatic
      - --path.settings=/usr/share/logstash/config
      command:
      - /bin/sh
      - /usr/local/bin1/rm_jndi.sh
      env:
      - name: SERVICENAME
        value: logstash
      - name: LOGSTASH_TYPE
```

在volumeMounts下增加映射目录：

- mountPath: /usr/local/bin1/
  name: rm-jdni



在volumes下增加挂载目录：

- hostPath:
  path: /opt/matrix/app/data/base-service/log-center/logstash
  type: ""
  name: rm-jdni

附件下载： rm_jdni.zip