

Apache Log4j2 升级替换说明

1. 漏洞说明

12月9日，绿盟科技 CERT 监测到网上披露 Apache Log4j2 远程代码执行漏洞，由于 Apache Log4j2 某些功能存在递归解析功能，未经身份验证的攻击者通过发送特别构造的数据请求包，可在目标服务器上执行任意代码。漏洞 PoC 已在网上公开，默认配置即可进行利用，该漏洞影响范围极广，建议相关用户尽快采取措施进行排查与防护。

受影响的是 log4j-core-*.jar，受影响版本：

Apache Log4j 2.x <= 2.14.1

2. 排查当前产品包依赖的 log4j jar 是否需要升级

首先，对照如下表格排查您所使用的超图云产品版本依赖的 log4j jar 是否需要升级，如需升级，请参照后续教程，替换产品包中的 log4j jar。

产品名称	版本	依赖的log4j jar情况	是否需要升级	升级后的log4j版本
iServer	9.1.0	log4j-api-2.8.2.jar log4j-core-2.9.1.jar	是	log4j-api-2.17.0.jar log4j-core-2.17.0.jar
	9.1.1	log4j-api-2.8.2.jar log4j-core-2.9.1.jar	是	log4j-api-2.17.0.jar log4j-core-2.17.0.jar
	9.1.2	log4j-1.2.17.jar log4j-api-2.8.2.jar	否	——
	10.1.3	log4j-1.2.17.jar log4j-api-2.13.2.jar	否	——
	10.1.4	log4j-1.2-api-2.14.1.jar log4j-api-2.14.1.jar log4j-core-2.14.1.jar	是	log4j-1.2-api-2.17.0.jar log4j-api-2.17.0.jar log4j-core-2.17.0.jar
	10.2.0	log4j-1.2.17.jar log4j-api-2.14.1.jar	否	——
iEdge	9.1.0	log4j-api-2.8.2.jar log4j-core-2.9.1.jar	是	log4j-api-2.17.0.jar log4j-core-2.17.0.jar
	9.1.1	log4j-api-2.8.2.jar log4j-core-2.9.1.jar	是	log4j-api-2.17.0.jar log4j-core-2.17.0.jar
	9.1.2	log4j-api-2.8.2.jar log4j-core-2.9.1.jar	是	log4j-api-2.17.0.jar log4j-core-2.17.0.jar
	10.1.3	log4j-1.2.17.jar log4j-api-2.13.2.jar	否	——
	10.1.4	log4j-1.2-api-2.14.1.jar log4j-api-2.14.1.jar log4j-core-2.14.1.jar	是	log4j-1.2-api-2.17.0.jar log4j-api-2.17.0.jar log4j-core-2.17.0.jar
	10.2.0	log4j-1.2.17.jar log4j-api-2.14.1.jar	否	——
iPortal	9.1.0	log4j-api-2.8.2.jar log4j-core-2.9.1.jar	是	log4j-api-2.17.0.jar log4j-core-2.17.0.jar
	9.1.1	log4j-api-2.8.2.jar log4j-core-2.9.1.jar	是	log4j-api-2.17.0.jar log4j-core-2.17.0.jar
	9.1.2	log4j-1.2.17.jar log4j-api-2.8.2.jar	否	——
	10.1.3	log4j-api-2.13.2.jar log4j-core-2.13.2.jar	是	log4j-api-2.17.0.jar log4j-core-2.17.0.jar
	10.1.4	log4j-1.2-api-2.14.1.jar log4j-api-2.14.1.jar log4j-core-2.14.1.jar	是	log4j-1.2-api-2.17.0.jar log4j-api-2.17.0.jar log4j-core-2.17.0.jar
	10.2.0	log4j-api-2.14.1.jar log4j-core-2.13.2.jar	是	log4j-api-2.17.0.jar log4j-core-2.17.0.jar

注：如果您使用的是临时包，或不知道当前使用的云产品版本，也不知道是否需要升级 Log4j 时，您可以在软件包安装目录中搜索 log4j 关键字，如果搜索到 log4j-core-2.*.jar <= 2.14.1，则表明您的产品包需要升级 log4j。log4j-1.*.jar 不受影响。

3. 替换产品包依赖的 log4j jar

如您排查出产品包依赖的 log4j jar 需要升级，请参照表格替换原有的 log4j jar 包。下面以 iPortal 10.1.4 版本为例，为您介绍如何替换产品包中的 log4j jar 包：

- (a) 停止 iPortal 进程；
- (b) 进入 %SuperMap iPortal_HOME%\webapps\iportal\WEB-INF\lib 目录，删除如图所示的 log4j jar 包：

注：iServer 依赖的 log4j jar 包存放于 %SuperMap iServer_HOME%\webapps\iserver\WEB-INF\lib 目录；

iEdge 依赖的 log4j jar 包存放于 %SuperMap iEdge_HOME%\webapps\iserver\WEB-INF\lib 目录；

> test > 1014 > supermap-iportal-10.1.4-win64-deploy > webapps > iportal > WEB-INF > lib

名称	修改日期	类型	大小
lang-mustache-client-6.8.15.jar	2021/7/28 12:20	JAR 文件	61 KB
lang-tag-1.5.jar	2021/7/28 12:35	JAR 文件	11 KB
license-client-lib-deploy-10.1.0-20201216...	2021/11/19 14:37	JAR 文件	86 KB
listenablefuture-9999.0-empty-to-avoid-co...	2021/7/28 12:20	JAR 文件	3 KB
log4j-1.2-api-2.14.1.jar	2021/11/3 11:44	JAR 文件	202 KB
log4j-api-2.14.1.jar	2021/9/8 14:14	JAR 文件	294 KB
log4j-core-2.14.1.jar	2021/11/3 11:44	JAR 文件	1,705 KB
log4s_2.11-1.8.2.jar	2021/7/28 12:21	JAR 文件	69 KB
lucene-analyzers-common-7.7.3.jar	2021/7/28 12:20	JAR 文件	1,626 KB
lucene-backward-codecs-7.7.3.jar	2021/7/28 12:20	JAR 文件	98 KB
lucene-core-7.7.3.jar	2021/7/28 12:20	JAR 文件	3,018 KB
lucene-grouping-7.7.3.jar	2021/7/28 12:20	JAR 文件	86 KB

- (c) 参照表格说明，将产品包中升级需要的 log4j jar 包，从本压缩包中复制到 lib 目录下，完成替换。

> 软件 (D:) > log4j2.17

名称	修改日期	类型	大小
log4j-1.2-api-2.17.0.jar	2021/12/24 15:37	JAR 文件	204 KB
log4j-api-2.17.0.jar	2021/12/24 15:37	JAR 文件	295 KB
log4j-core-2.17.0.jar	2021/12/24 15:37	JAR 文件	1,748 KB