

# 2022-03-25 -CVE-2016-10750-远程代码执行

|        |                                 |
|--------|---------------------------------|
| 主题     | CVE-2016-10750 Hazelcast 远程代码执行 |
| 公告发布日期 | 2022-03-25                      |
| 影响产品   |                                 |
| CVE ID |                                 |

## 说明

Atlassian安全团队目前正在调查Log4j远程代码执行漏洞（CVE-2021-44228）的影响，并确定对我们的本地产品的任何可能影响。

到目前为止，我们认为我们的本地部署产品在其默认配置中不易受到攻击。但是，如果您修改了默认日志记录配置（log4j.properties）并启用JMS Appender功能，则可以在以下产品中远程执行代码：

- Jira Server & Data Center
- Confluence Server & Data Center
- Bamboo Server & Data Center
- Crowd Server & Data Center
- Fisheye
- Crucible

我们可以通过检查Log4j配置文件来检查是否存在漏洞。如果找到包含配置项org.apache.log4j.net.JMSAppender那么它可能会受到影响  
我们建议将它进行屏蔽。

## 临时防范

- 增加修改 jvm 参数 -Dlog4j2.formatMsgNoLookups=true
- 修改配置 log4j2.formatMsgNoLookups=True
- 将系统环境变量 FORMAT\_MESSAGES\_PATTERN\_DISABLE\_LOOKUPS 设置为true

## 各产品log4j配置文件

| 产品                              | 默认路径                                                                                                                                                                                                                                  |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jira Server & Data Center       | <install-directory>/atlassian-jira/WEB-INF/classes/log4j.properties                                                                                                                                                                   |
| Confluence Server & Data Center | <install-directory>/confluence/WEB-INF/classes/log4j.properties                                                                                                                                                                       |
| Bamboo Server & Data Center     | <install-directory>/atlassian-bamboo/WEB-INF/classes/log4j.properties                                                                                                                                                                 |
| Fisheye / Crucible              | <install-directory>/log4j.xml                                                                                                                                                                                                         |
| Crowd                           | <install-directory>/crowd-webapp/WEB-INF/classes/log4j.properties<br><install-directory>/crowd-openidclient-webapp/WEB-INF/classes/log4j.properties<br><install-directory>/crowd-openidserver-webapp/WEB-INF/classes/log4j.properties |

## Bitbucket

目前不受影响

Bitbucket的日志组件使用的logback, 具体可参见：<http://logback.qos.ch/>

如果不放心，可以将log4j的几个jar包替换掉

- 步骤一

将安装目录下的app/WEB-INF/lib中的四个文件删除掉

- 步骤二

将附件中的4个文件更新安装目录app/WEB-INF/lib下

| File                                          | Modified  |
|-----------------------------------------------|----------------------------------------------------------------------------------------------|
| Java Archive log4j-to-slf4j-2.15.0.jar        | 2022-03-29 by 红旗公                                                                            |
| Java Archive log4j-api-2.15.0.jar             | 2022-03-29 by 红旗公                                                                            |
| Java Archive log4j-core-2.15.0.jar            | 2022-03-29 by 红旗公                                                                            |
| Java Archive log4j-over-slf4j-1.8.0-beta4.jar | 2022-03-29 by 红旗公                                                                            |

 [Download All](#)