Apache Log4j 多个高危漏洞完整处置手册

■ **通告编号** **NS-2021-0045-10**	■ 发布日期 **2021-12-16**
■ **漏洞危害** **攻击者利用漏洞，可实现远程代码执行与拒绝服务攻击。**	
■ **TAG** Log4j、JNDI、CVE-2021-44228、CVE-2021-4104、CVE-2021-45046	

一. 漏洞概述

12 月 9 日，绿盟科技 CERT 监测到网上披露 Apache Log4j 远程代码执行漏洞（CVE-2021-44228），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。

12 月 10 日，绿盟科技 CERT 发现 Apache Log4j 2.15.0-rc1 版本仅修复 LDAP 和增加了 host 白名单，非默认配置下可以被绕过利用；官方对此发布了 Apache Log4j 2.15.0-rc2 版本（与 2.15.0 稳定版相同）进行修复，增加了对 url 异常的处理。

12 月 12 日，官方又发布了 Apache Log4j 2.15.1-rc1 版本，在默认配置中禁用了 JNDI 和 Message lookups 功能。

12 月 13 日，官方再发布了 Apache Log4j 2.16.0-rc1（与 2.16.0 稳定版相同）版本，此版本在 2.15.1-rc1 的基础上，移除掉了存在漏洞的 Message lookups 功能。

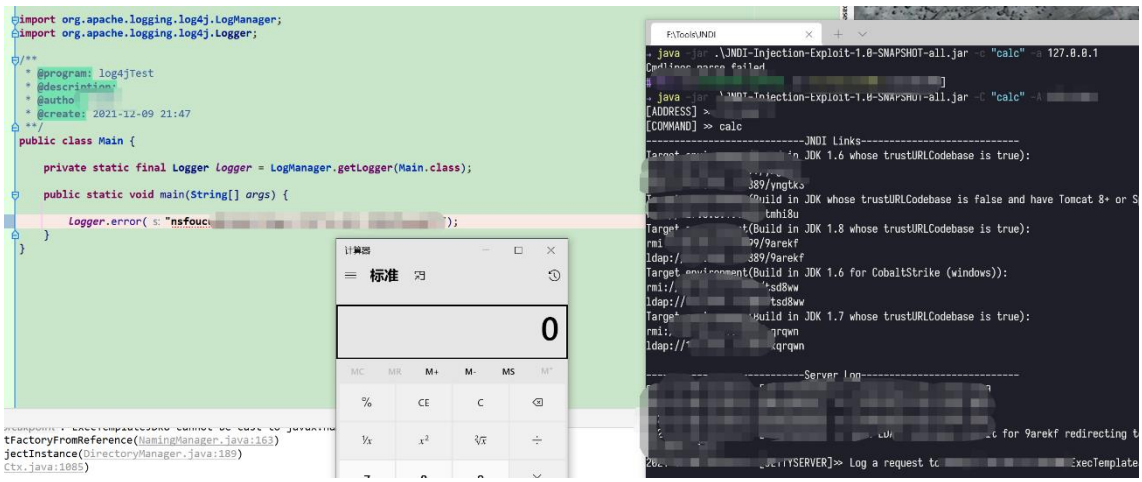
12 月 14 日，官方发布通告，披露 Apache Log4j 1.2.x 版本在特定配置时存在 JMSAppender 反序列化代码执行漏洞（CVE-2021-4104），当攻击者具有修改 Log4j 配置的权限时，JMSAppender 容易受到不可信数据的反序列化，攻击者可以使用特定配置利用 JMSAppender 执行 JNDI 请求，从而造成远程代码执行。

12 月 14 日，官方发布了 Apache Log4j 2.12.2-rc1（与 2.12.2 稳定版相同）版本，默认配置禁用了 JNDI，并移除掉存在漏洞的 Message lookups 功能，此版本支持 Java 7。

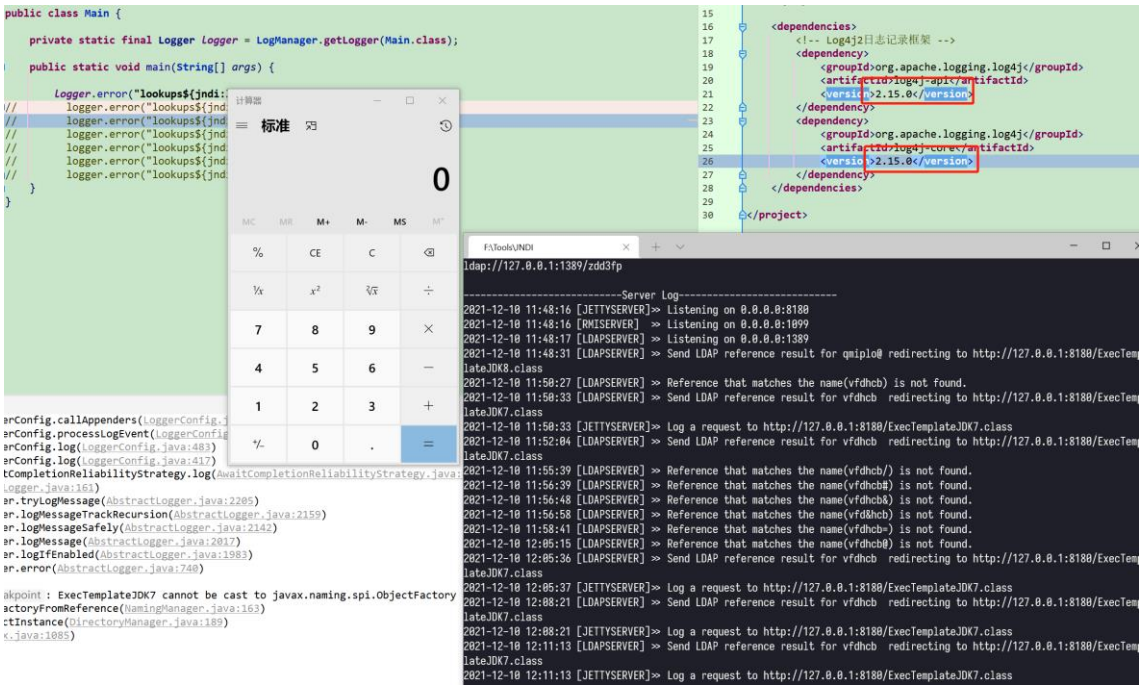
12 月 15 日，官方发布通告，披露 Apache Log4j 的 DoS 漏洞（CVE-2021-45046），当 log4j 配置使用非默认模式布局和上下文查找（例如$${ctx:loginId}）或线程上下文映射模式（%X、%mdc 或%MDC）时，使用 JNDI 查找模式制作恶意输入数据从而导致拒绝服务(DoS) 攻击。Apache Log4j 2.15.0 版本中针对 CVE-2021-44228 的漏洞修复方式不完善，在特定配置时受此漏洞影响。

Apache Log4j2 是一款开源的 Java 日志框架，被广泛地应用在中间件、开发框架与 Web 应用中，用来记录日志信息。

CVE-2021-44228 漏洞复现截图：



CVE-2021-44228 在 2.15.0-rc1 绕过复现截图：



CVE-2021-44228 漏洞状态：

漏洞细节	漏洞 PoC	漏洞 EXP	在野利用
已公开	已公开	已公开	存在

参考链接：

https://logging.apache.org/log4j/2.x/security.html

https://www.mail-archive.com/announce@apache.org/msg06925.html

https://www.mail-archive.com/announce@apache.org/msg06936.html

二. 影响范围

受影响版本

CVE-2021-44228：

- 2.0-beta9 <= Apache Log4j <= 2.12.1
- 2.13.0<= Apache Log4j <= 2.15.0-rc1

CVE-2021-45046：

- 2.0-beta9 <= Apache Log4j <= 2.12.1
- 2.13.0<= Apache Log4j <= 2.15.0-rc2（2.15.0 稳定版）

注：只有 log4j-core jar 文件受此漏洞影响。

CVE-2021-4104：

- Apache Log4j =1.2.x

供应链影响范围：

经不完全统计，直接和间接引用 Log4j 的开源组件共计超过 17 万个；

log4j 的 1～4 层引用关系：直接引用 log4j 的组件有 6960 个，第二层引用的超过 3 万个，第三层超过 9 万个，第四层超过 16 万个，总计有 173200+个开源组件受 Log4j 漏洞影响。

已知受影响应用及组件：

VMware 大部分产品

Jedis

Logging

Logstash

HikariCP

Hadoop Hive

ElasticSearch

Apache Solr

Apache Struts2

Apache Flink

Apache Druid

Apache Log4j SLF4J Binding

spring-boot-strater-log4j2

Camel :: Core

JBoss Logging 3

JUnit Vintage Engine

WSO2 Carbon Kernel Core

直接引用 log4j 的组件可参考如下链接：

https://mvnrepository.com/artifact/org.apache.logging.log4j/log4j-core/usages?p=1

不受影响版本

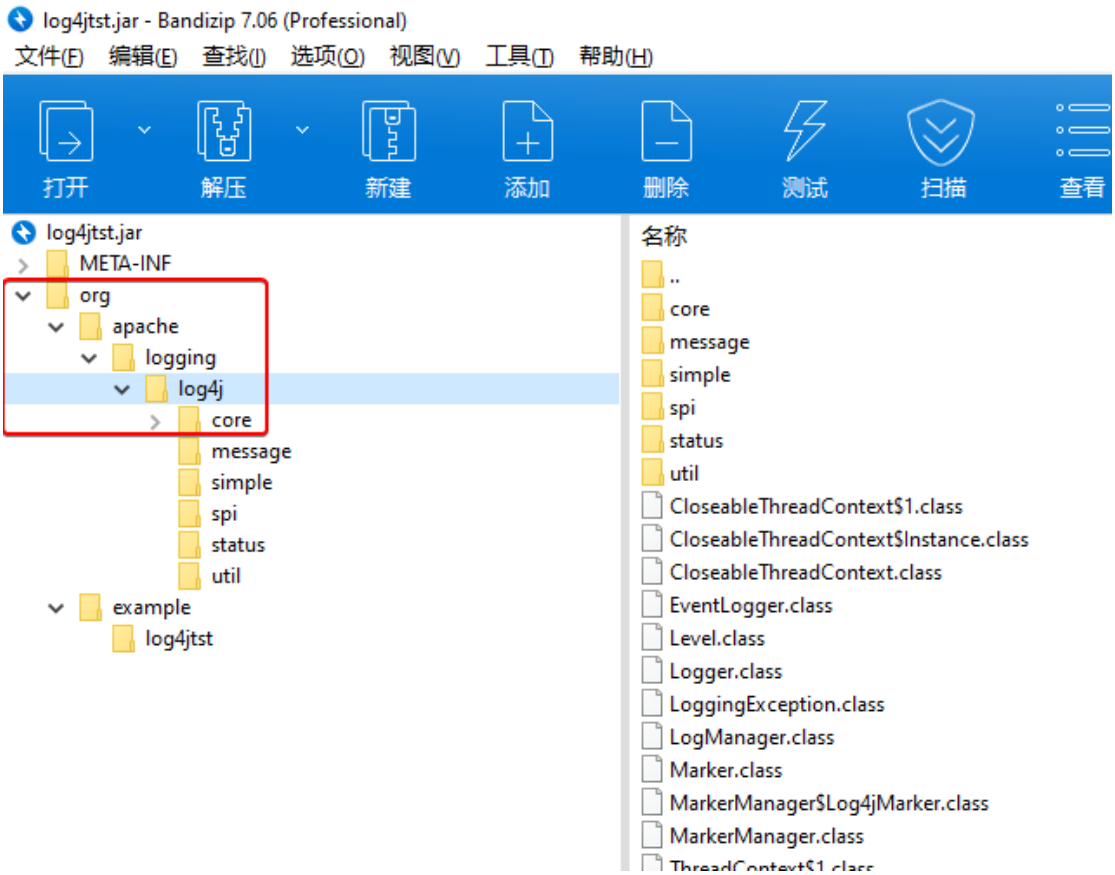
- Apache Log4j 2.15.1-rc1
- Apache Log4j 2.16.0-rc1（与 2.16.0 稳定版相同）
- Apache Log4j 2.12.2-rc1（与 2.12.2 稳定版相同）

注：Apache Log4j 2.12.2 支持 Java 7

三. 漏洞检测

3.1 人工检测

1、相关用户可根据 Java jar 解压后是否存在 org/apache/logging/log4j 相关路径结构，判断是否使用了存在漏洞的组件，若存在相关 Java 程序包，则很可能受漏洞影响。



2、若程序使用 Maven 打包，可查看项目的 pom.xml 文件中是否存在下图所示的相关字段，若版本号为小于 2.15.1，则应用受漏洞影响。

pom.xml (log4jtst) | Main.java | log4j2.xml | log4j2.component.properties

```
9       <version>1.0-SNAPSHOT</version>
10
11      <properties>
12          <maven.compiler.source>8</maven.compiler.source>
13          <maven.compiler.target>8</maven.compiler.target>
14      </properties>
15
16      <dependencies>
17          <dependency>
18              <groupId>org.apache.logging.log4j</groupId>
19              <artifactId>log4j-api</artifactId>
20              <version>2.12.1</version>
21          </dependency>
22          <dependency>
23              <groupId>org.apache.logging.log4j</groupId>
24              <artifactId>log4j-core</artifactId>
25              <version>2.12.1</version>
26          </dependency>
27      </dependencies>
```

3、若程序使用 gradle 打包，可查看 build.gradle 编译配置文件，若在 dependencies 部分存在 org.apache.logging.log4j 相关字段，且版本号为小于 2.15.1，则应用受漏洞影响。

```
dependencies {
  compile group: 'org.apache.logging.log4j', name: 'log4j-api', version: '2.14.1'
  compile group: 'org.apache.logging.log4j', name: 'log4j-core', version: '2.14.1'
}
```

3.2 攻击排查

1、攻击者在利用漏洞前通常采用 dnslog 方式进行扫描、探测，常见的漏洞利用方式可通过应用系统报错日志中的"javax.naming.CommunicationException"、"javax.naming.NamingException: problem generating object using object factory"、"Error looking up JNDI resource"关键字进行排查。

```
R:\Temp\log4jt\out\artifacts\log4jtst_jar>java -jar log4jtst.jar
Unable to get Charset 'cp65001' for property 'sun.stdout.encoding', using default GBK and continuing.
01:11:35.062 [main] ERROR org.example.log4jtst.Main - Hello World
2021-12-10 01:11:40,814 main WARN Error looking up JNDI resource [ldap://[redacted].ceye.io]. javax.naming.Communicat
ionException: [redacted].ceye.io:389 [Root exception is java.net.ConnectException: Connection refused: connect]
        at com.sun.jndi.ldap.Connection.<init>(Connection.java:238)
        at com.sun.jndi.ldap.LdapClient.<init>(LdapClient.java:137)
        at com.sun.jndi.ldap.LdapClient.getInstance(LdapClient.java:1609)
        at com.sun.jndi.ldap.LdapCtx.connect(LdapCtx.java:2749)
        at com.sun.jndi.ldap.LdapCtx.<init>(LdapCtx.java:319)
        at com.sun.jndi.url.ldap.ldapURLContextFactory.getUsingURLIgnoreRootDN(ldapURLContextFactory.java:60)
        at com.sun.jndi.url.ldap.ldapURLContext.getRootURLContext(ldapURLContext.java:61)
        at com.sun.jndi.toolkit.url.GenericURLContext.lookup(GenericURLContext.java:202)
        at com.sun.jndi.url.ldap.ldapURLContext.lookup(ldapURLContext.java:94)
        at javax.naming.InitialContext.lookup(InitialContext.java:417)
        at org.apache.logging.log4j.core.net.JndiManager.lookup(JndiManager.java:172)
        at org.apache.logging.log4j.core.lookup.JndiLookup.lookup(JndiLookup.java:56)
        at org.apache.logging.log4j.core.lookup.Interpolator.lookup(Interpolator.java:198)
        at org.apache.logging.log4j.core.lookup.StrSubstitutor.resolveVariable(StrSubstitutor.java:1060)
```

2、攻击者发送的数据包中可能存在"${jndi:}" 字样，推荐使用全流量或 WAF 设备进行检索排查。

3.3 产品检测

绿盟科技远程安全评估系统（RSAS）与 WEB 应用漏洞扫描系统(WVSS)、工控漏洞扫描系统（ICSScan）、网络入侵检测系统（IDS）、综合威胁探针（UTS）已具备对 CVE-2021-44228 漏洞的扫描与检测能力，请有部署以上设备的用户升级至最新版本。

	升级包版本号	升级包下载链接
RSAS V6 系统插件包	V6.0R02F01.2510 信创： V6.0R02F01.1704	http://update.nsfocus.com/update/downloads/id/122199 信创： http://update.nsfocus.com/update/downloads/id/122003
RSAS V6 Web 插件包	V6.0R02F00.2409	http://update.nsfocus.com/update/downloads/id/122201

WVSS V6 插件升级包	V6.0R03F00.235	http://update.nsfocus.com/update/downloads/id/122203
ICSScan V6.0 系统插件包	V6.0R00F04.2405	http://update.nsfocus.com/update/downloads/id/122116
ICSScan V6.0 Web 插件包	V6.0R00F04.2306	http://update.nsfocus.com/update/downloads/id/122127
IDS	5.6.11.26706	http://update.nsfocus.com/update/downloads/id/122010
	5.6.10.26706	http://update.nsfocus.com/update/downloads/id/122009
	5.6.9.26706	http://update.nsfocus.com/update/downloads/id/122008
UTS	5.6.10.26706	http://update.nsfocus.com/update/downloads/id/122103

关于 RSAS 的升级配置指导，请参考如下链接：

https://mp.weixin.qq.com/s/SgOaCZeKrNn-4uR8Yj_C3Q

3.4 申请云检测

绿盟科技面向用户提供远程检测服务，因该漏洞的检测存在一定风险，相关客户如需要申请云检测，请联系销售或项目经理沟通，或用个人的公司邮箱发邮件至 rs@nsfocus.com，在正文中提供需要扫描的资产清单，可以扫描的时间，联系方式，服务人员会与您联系。

7x24h 客服咨询热线：400-818-6868 转 2

四. 漏洞防护

4.1 官方升级

目前官方已针对上述漏洞发布多个修复版本，不同版本更新内容略有不同，受影响用户可根据不同需求选择对应的版本升级，下载链接：https://github.com/apache/logging-log4j2/t

ags

Apache Log4j 版本号	版本更新说明
Apache Log4j 2.15.0-rc1	修复了 LDAP 和增加 host 白名单，手动开启 Lookup 功能时可被绕过，且存在 DoS 攻击漏洞（CVE-2021-45046）
Apache Log4j 2.15.0-rc2	增加了对 url 异常的处理，进一步修复 CVE-2021-44228 漏洞。但存在 DoS 攻击漏洞（CVE-2021-45046）
Apache Log4j 2.15.0 稳定版	增加了对 url 异常的处理，进一步修复 CVE-2021-44228 漏洞。但存在 DoS 攻击漏洞（CVE-2021-45046）
Apache Log4j 2.15.1-rc1	默认配置禁用了 JNDI 和 Message lookups 功能。
Apache Log4j 2.16.0-rc1	默认配置禁用 JNDI 功能，并完全移除 Message lookups 功能
Apache Log4j 2.16.0 稳定版	默认配置禁用 JNDI 功能，并完全移除 Message lookups 功能
Apache Log4j 2.12.2-rc1	默认配置禁用 JNDI 功能，并完全移除 Message lookups 功能，该版本支持 Java7。
Apache Log4j 2.12.2 稳定版	默认配置禁用 JNDI 功能，并完全移除 Message lookups 功能，该版本支持 Java7。

注：1、官方在 Apache Log4j 2.15.0-rc1 版本中已将 log4j2.formatMsgNoLookups 默认设置为 true，在不手动开启 Lookup 的情况下，Log4j 2.15.0-rc1 版本不受 CVE-2021-44228 漏洞的影响。

2、建议受影响用户将 Apache Log4j 所有相关应用升级到 ApacheLog4j2.15.1-rc1（测试版）或 Apache Log4j 2.16.0（稳定版）。

3、推荐优先选择稳定版升级，Java 7 环境的用户可升至 Apache Log4j 2.12.2 修复。

4、防止升级过程出现意外，建议相关用户在备份数据后再进行操作。

5、升级供应链中已知受影响的应用及组件：见前文《二、影响范围》的供应链影响范围。

4.2 产品防护

针对 CVE-2021-44228 漏洞，绿盟科技网络入侵防护系统(IPS)、WEB 应用防护系统(WAF)与下一代防火墙 (NF)已发布规则升级包，请相关用户升级规则包至最新版，以形成安全产品防护能力。安全防护产品规则版本号如下：

安全防护产品	规则版本号	升级包下载链接	规则编号

IPS	5.6.11.26706	http://update.nsfocus.com/update/downloads/id/122010	[25475]
	5.6.10.26706	http://update.nsfocus.com/update/downloads/id/122009	
	5.6.9.26706	http://update.nsfocus.com/update/downloads/id/122008	
WAF	6.0.7.3.52185	http://update.nsfocus.com/update/downloads/id/122193	27005085
	6.0.7.0.52185	http://update.nsfocus.com/update/downloads/id/122194	
NF	6.0.1.863	http://update.nsfocus.com/update/downloads/id/122048	25476
	6.0.2.863	http://update.nsfocus.com/update/downloads/id/122049	
	6.0.60.863	http://update.nsfocus.com/update/downloads/id/122045	
	6.0.70.863	http://update.nsfocus.com/update/downloads/id/122047	

产品规则升级的操作步骤详见如下链接：

IPS：https://mp.weixin.qq.com/s/DxQ3aaap8aujqZf-3VbNJg

WAF：https://mp.weixin.qq.com/s/7F8WCzWsuJ5T2E9e01wNog

NF：https://mp.weixin.qq.com/s/R3k_KJm4O52bxy794jjo4A

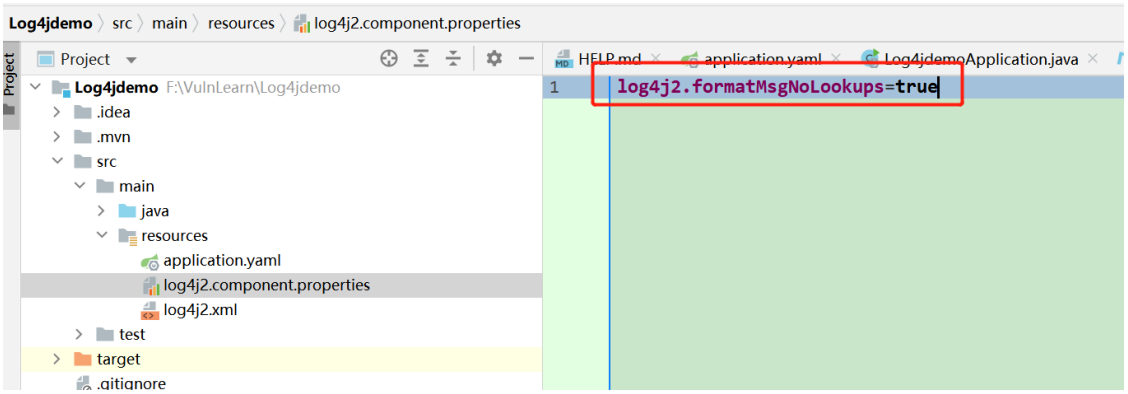
4.3 临时防护措施

若相关用户暂时无法进行升级操作，可先用下列措施对上述漏洞进行临时缓解：

Apache Log4j 远程代码执行漏洞（CVE-2021-44228）临时防护：

1、添加 jvm 参数启动：-Dlog4j2.formatMsgNoLookups=true

2、在应用的 classpath 下添加 log4j2.component.properties 配置文件，文件内容为：log4j2.formatMsgNoLookups=true



3、设置系统环境变量 LOG4J_FORMAT_MSG_NO_LOOKUPS=true

4、使用下列命令，移除 log4j-core 包中的 JndiLookup 类文件：

```
zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

注：当且仅当 Apache Log4j >= 2.10 版本时，可使用 1、2、3、4 的任一措施进行防护。

5、Apache Log4j 2.7 及以上的版本，可在 PatternLayout 配置中使用%m{nolookups}对漏洞进行缓解。

6、采用人工方式禁用 JNDI，例：在 spring.properties 中添加 spring.jndi.ignore=true

7、建议使用 JDK 在 11.0.1、8u191、7u201、6u211 及以上的高版本，可在一定程度上缓解代码执行的利用。

8、限制受影响应用对外访问互联网，并在边界对 dnslog 相关域名的访问进行检测。

部分公共 dnslog 平台如下：

ceye.io

dnslog.link

dnslog.cn

dnslog.io

tu4.org

burpcollaborator.net

s0x.cn

Apache Log4j JMSAppender 反序列化代码执行漏洞（CVE-2021-4104）临时防护：

1）注释掉或删除 Log4j 配置中的 JMSAppender。

2）使用下列命令，从 log4j jar 包中删除 JMSAppender 类文件：

```
zip  -q  -d  log4j-*.jar  org/apache/log4j/net/JMSAppender.class
```

3）限制系统用户对应用程序平台的访问，以防止攻击者修改 Log4j 的配置。

Apache Log4j DoS 漏洞（CVE-2021-45046）临时防护：

使用下列命令，移除 log4j-core 包中的 JndiLookup 类文件：

```
zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

4.4 平台监测

绿盟安全管理平台（ESP-H）与绿盟智能安全运营平台（ISOP）已经具备针对此漏洞的检测能力，部署有绿盟科技平台类产品的用户，可实现对 CVE-2021-44228 漏洞的平台监测能力。

安全平台	升级包/规则版本号
ESP-H（绿盟安全管理平台）	使用最新规则升级包 attack_rule.1.0.0.1.1048648.dat
ISOP（绿盟智能安全运营平台）	升级攻击识别规则包至最新 attack_rule.1.0.0.1.1048648.dat

声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。

绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。