# 附件四 漏洞报告样例

**Vulnerability Detection Report**

**漏洞检测报告**

**2023/04/04**

## 漏洞概况

您本次共检测出16个漏洞，经分析后得知，共有12种不同类型的漏洞。现将这些漏洞的基本信息整理成下方的表格：

|  |  |  |  |
| --- | --- | --- | --- |
| **CVE-ID** | **CWE-ID** | **披露时间** | **CVSS 3.x评分** |
| **CVE-2019-17564** | [CWE-502](http://cwe.mitre.org/data/definitions/502.html) | 04/01/2020 | 9.8 |
| **CVE-2020-1948** | CWE-502 | 07/14/2020 | 9.8 |
| **CVE-2020-9492** | CWE-863 | 01/26/2021 | 8.8 |
| **CVE-2021- 20180** | CWE-532 | 03/16/2022 | 5.0 |
| **CVE-2021-21686** | CWE-59,CWE-22 | 11/04/2021 | 8.1 |
| **CVE-2021-21687** | [CWE-862](http://cwe.mitre.org/data/definitions/862.html) | 11/04/2021 | 9.1 |
| **CVE-2021-22147** | CWE-862,CWE-732 | 08/03/2021 | 6.5 |
| **CVE-2021- 25640** | CWE-918 | 06/01/2021 | 6.1 |
| **CVE-2021-25641** | CWE-502 | 06/01/2021 | 9.8 |
| **CVE-2021- 30179** | CWE-502 | 06/01/2021 | 9.8 |
| **CVE-2021-30180** | CWE-444 | 06/01/2021 | 9.8 |
| **CVE-2021-30181** | NVD-CWE-noinfo | 06/01/2021 | 9.8 |
| **CVE-2021-30639** | CWE-755 | 07/26/2022 | 7.5 |
| **CVE-2021-43297** | CWE-502 | 01/10/2022 | 9.8 |
| **CVE-2021-44224** | [CWE-476](http://cwe.mitre.org/data/definitions/476.html) | 12/20/2021 | 8.2 |
| **CVE-2021-44790** | CWE-787 | 12/20/2021 | 9.8 |

* **漏洞信息**

以下是本次检测出来的所有漏洞的详细报告

**漏洞1**

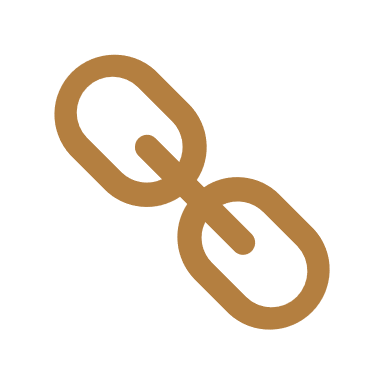
**漏洞信息**

* **漏洞编号**: CVE-2019-17564
* **平台**： NVD平台
* **链接**： <https://nvd.nist.gov/vuln/detail/CVE-2019-17564>
* **漏洞披露时间：** 04/01/2020
* **漏洞参考链接：**

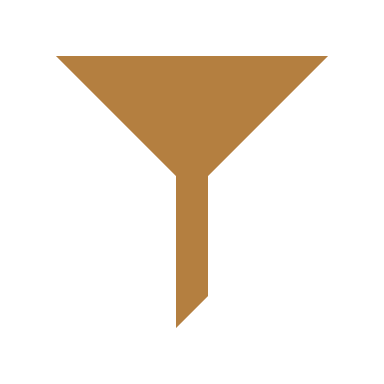
<https://cert.360.cn/report/detail?id=fdf2dd6ab0c6e39e18a725ea86ad66bb>

<https://github.com/fairyming/CVE-2019-17564>

<https://nvd.nist.gov/vuln/detail/CVE-2019-17564>

**在野漏洞报告**：

<https://www.cvedetails.com/cve/CVE-2021-21686>

**漏洞类型**：

*CWE-502*

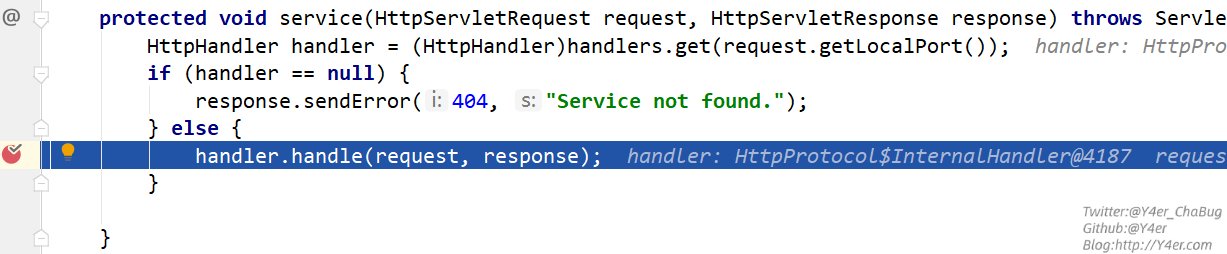
**漏洞危害**

* **漏洞严重性**：CVSS 3.x评分：9.8 CVSS 2.0 评分：6.8
* **影响版本**：Apache Dubbo 2.5.0 - 2.5.10；2.6.0 - 2.6.7 ；2.7.0 -2.7.4

**漏洞成因**

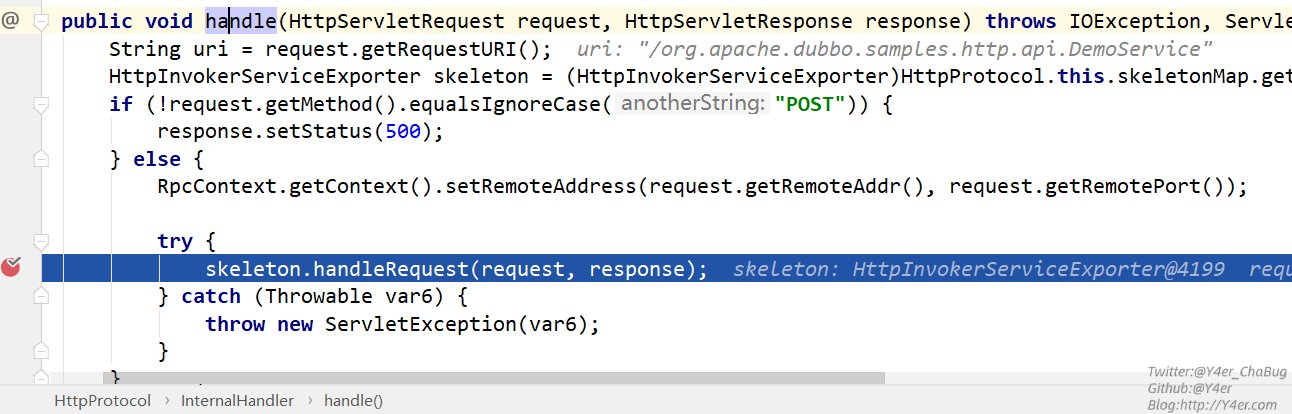
断点：dubbo-2.7.3.jar!/org/apache/d

ubbo/remoting/http/servlet/DispatcherServlet.class:43

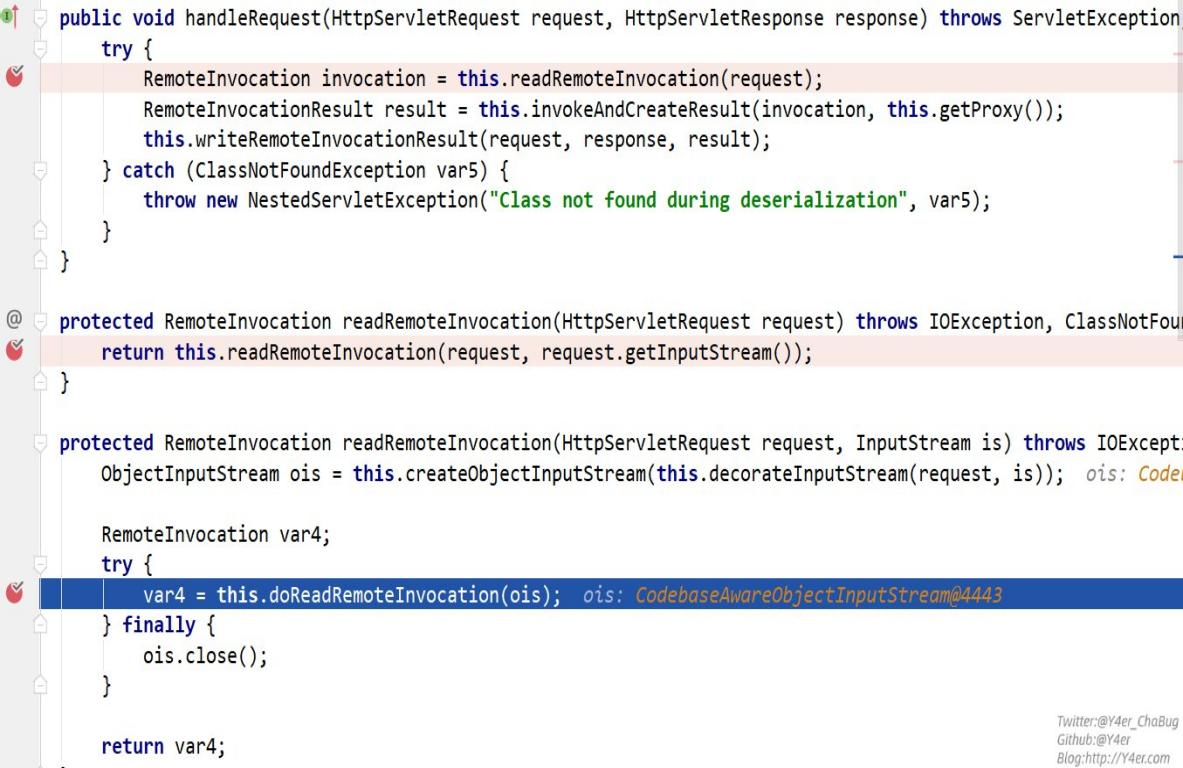
[](https://y4er.com/img/uploads/20200216172086.png)

跟进到 org.apache.dubbo.rpc.protocol.

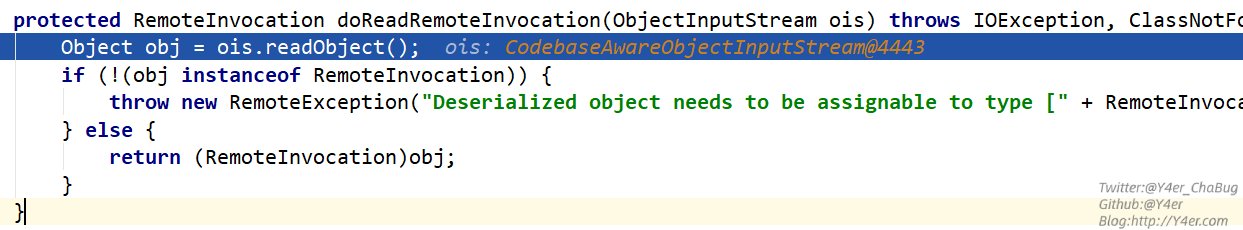
http.HttpProtocol.InternalHandler#handle

[](https://y4er.com/img/uploads/20200216178969.png)

获取了URI、请求方式和RPC调用的上下文，然后进入handleRequest()

[](https://y4er.com/img/uploads/20200216173990.png)

handleRequest()将request请求对象传入一个参数的readRemoteInvocation()，然后将request和request.getInputStream()传入其重载方法两个参数的readRemoteInvocation()，然后创建了ois对象，ois对象中包含了post请求的数据，然后进入doReadRemoteInvocation()

[](https://y4er.com/img/uploads/20200216177168.png)

到达readObject()，整个过程ois对象没有过滤，而ois中又包含了post报文，导致反序列化漏洞，如果存在可用的gadget，会导致RCE。

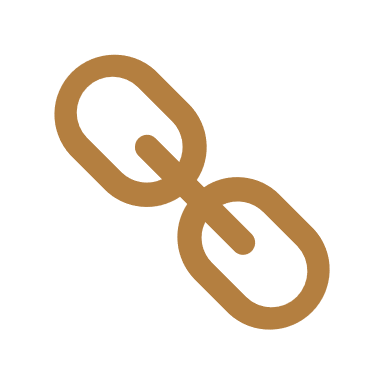
**漏洞治理**

|  |  |  |
| --- | --- | --- |
|  | | |
| 漏洞位置 | org.springframework.remoting.rmi.RemoteInvocationSerializing  Exporter#doReadRemoteInvocation第68行 | |
| 漏洞PoC | | <http://www.code2sec.com/cve-2019-17564-dubbo-httpxie-yi-fan-xu-lie-hua-lou-dong.html> |
| 漏洞补丁 | https://github.com/apache/dubbo/commit/  5e2c07c1dc3f945c6375cbeb021af30fa6d4ac31 | |
| 处置建议 | 建议更新至最新版本 | |
|  | | |

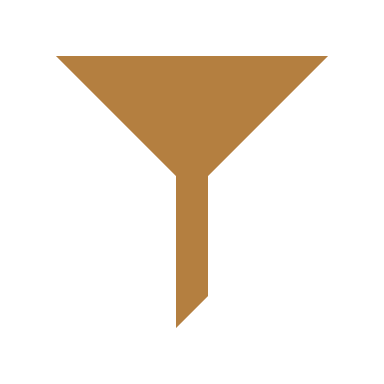
**漏洞2**

**漏洞信息**

* **漏洞编号**: CVE-2020-1948
* **平台**： NVD平台
* **链接**： https://nvd.nist.gov/vuln/detail/CVE-2020-1948
* **漏洞披露时间：** 07/14/2020

**在野漏洞报告**：

https://cloud.tencent.com/developer/article/1653754

**漏洞类型**：

*CWE-502*

**漏洞危害**

* **漏洞危害:**  不受信任数据的反序列化
* **漏洞严重性**：CVSS 3.x评分：9.8 CVSS 2.0 评分：7.5
* **影响版本**：Apache Dubbo 2.5.0 - 2.5.10 ； 2.6.0 - 2.6.7 ； 2.7.0 -2.7.4

**漏洞成因**

CVE-2020-1948远程代码执行漏洞原理是远程方法被动态调用导致的代码执行

本次漏洞利用的是 com.rometools.rome.feed.impl.ToStringBean#toString 方法，重写了 toString，该方法将会调用构造对象的所有 getter 方法。

执行 Dubbo 调用时，传入的是 ToStringBean 类型参数，构造的对象是com.sun.rowset.JdbcRowSetImpl，并且 datasource 属性设置的是 JNDI 暴露的 url，在调用 JdbcRowSetImpl 的 getDatabaseMetaData 方法时，执行 connect 操作，下载远端代码，在 Service Provider 执行，造成攻击。

调起 toString 方法的地方是在 Dubbo Provider 接收 DecodeHandler#received:44 请求，在 DecodeableRpcInvocation#decode 反序列化参数的地方：

dubbo 默认使用的是 hession2 序列化，解析参数执行的是这个方法org.apache.dubbo.common.serialize.hessian2.Hessian2ObjectInput#readUTF

在 hession 反序列化过程中，通过下面代码段执行到了 ToStringBean#toString

至此，注入攻击的流程到这里执行完成。

**漏洞治理**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| 漏洞位置 | | dubbo-rpc/dubbo-rpc-api/src/main/java/org/apache/  dubbo/rpc/support/RpcUtils.java第179~180行，第183~184行 | |
| 漏洞PoC | <https://www.cnblogs.com/JingQ/p/13329083.html> | |
| 漏洞补丁 | | <https://github.com/apache/dubbo/commit/5ad>  186fa874d9f0dfb87b989e54c1325d39abd40 | |
| 处置建议 | | 建议更新至最新版本 | |
| 漏洞3  漏洞信息   * 漏洞编号: CVE-2020-9492 * 平台： CVE/NVD * 链接： <https://nvd.nist.gov/vuln/detail/CVE-2020-9492> * 漏洞披露时间: 01/26/2021   筛选漏洞类型：  *CWE-863 权限提升漏洞*    聊天漏洞描述：  在 Apache Hadoop 3.2.0 到 3.2.1、3.0.0-alpha1 到 3.1.3 和 2.0.0-alpha 到 2.10.0 中，WebHDFS 客户端可能会在没有正确验证的情况下将 SPNEGO 授权标头发送到远程 URL。  漏洞危害  漏洞评级：8.8HIGH  影响版本（网站）：  Apache hadoop 2.0.0 - 2.10.0 (已在其他报告中验证)  Apache hadoop 3.0.0 - 3.1.3  Apache hadoop 3.2.0 - 3.2.1  Apache solr 8.6.0  Apache solr 8.6.2  Oracle financial\_services\_crime\_and\_compliance\_management\_studio 8.0.8.2.0 , 8.0.8.3.0  漏洞成因  在Apache hadoop中发现一个缺陷。WebHDFS客户端可以向远程URL发送SPNEGO授权头，而不需要适当的验证，这可能导致访问限制的绕过。这个漏洞的最大威胁是数据的保密性和完整性以及系统的可用性。  漏洞治理   |  | | | --- | --- | | **漏洞位置** | hadoop-hdfs-project/hadoop-hdfs-client/src/main/java /org/apache/hadoop/hdfs/web/WebHdfsFileSystem.java | | | **漏洞补丁** | N/A | | | **修复版本** | Apache hadoop 2.10.1  Apache hadoop 3.1.4  Apache hadoop 3.2.2 | | | **处置建议** | 1.设置不同的http签名机密，并使用专用主机进行每个权限模拟服务（如HiveServer2）。  2.升级到3.3.0、3.2.2、3.1.4、2.10.1或更新的TLS加密版本，启用并将dfs.http.policy配置为HTTPS\_ONLY。 | | | **参考链接** | [https://github.com/apache/hadoop/commit/](https://github.com/apache/hadoop/commit/81d8a887b0406380e469c76ed2e41022a6372dd7)  [81d8a887b0406380e469c76ed2e41022a6372dd7](https://github.com/apache/hadoop/commit/81d8a887b0406380e469c76ed2e41022a6372dd7) | | |  | | | | | | | |

# 漏洞4

## 漏洞信息

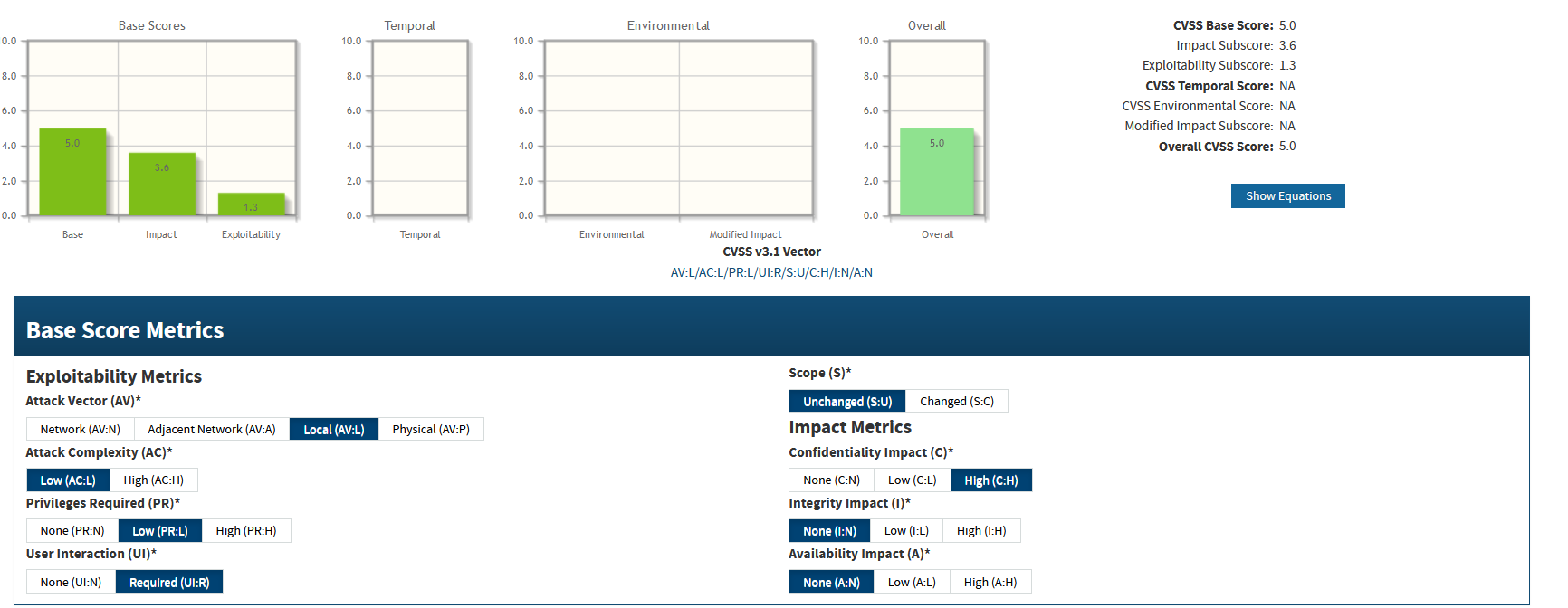
* **漏洞编号**: CVE-2021-20180
* **平台**： CVE/NVD
* **链接**： <https://nvd.nist.gov/vuln/detail/CVE-2021-20180>
* **漏洞披露时间**: 03/16/2022

**漏洞描述**：

在 ansible 模块中发现了一个缺陷，默认情况下，凭据在控制台日志中公开，并且在使用 bitbucket\_pipeline\_variable 模块时不受安全功能的保护。此缺陷允许攻击者窃取 bitbucket\_pipeline 凭据。此漏洞的最大威胁是与机密性有关。

## 漏洞危害

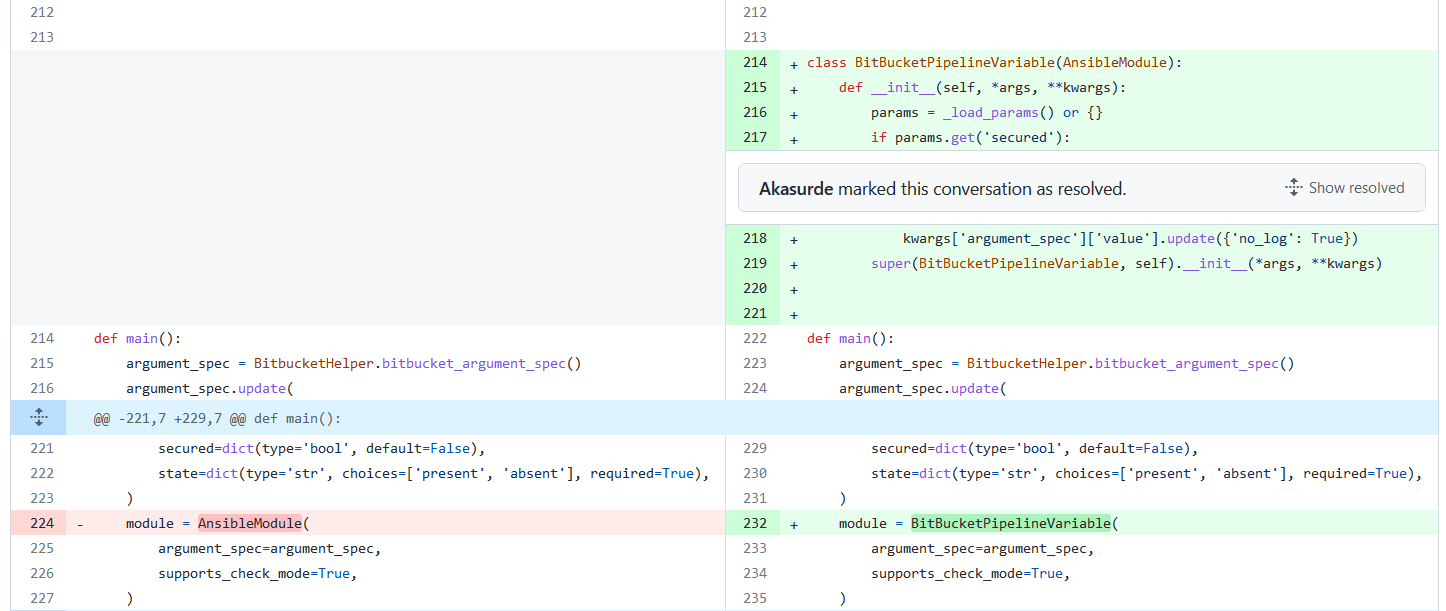
CVSS评分: 5.5 (NVD评分)，重新评价后: 5.0



漏洞影响的组件版本:

Redhat ansible 2.9.18之前的版本

经过验证，在2.9.18版本加入了隐藏标记为安全的用户敏感信息的代码：



在之前的版本都没有，详细代码见漏洞补丁一栏。

## 漏洞成因

默认情况下，凭据在控制台日志中公开，并且在使用 bitbucket\_pipeline\_variable 模块时不受安全功能的保护。此缺陷允许攻击者窃取 bitbucket\_pipeline 凭据。Red Hat Gluster Storage 3 中提供的 Ansible 版本不包含易受攻击的 bitbucket 模块，不受此漏洞影响。但是，Red Hat Gluster Storage 3 不再维护自己的 Ansible 版本。先决条件是启用 Ansible 存储库，以便使用最新版本的 Ansible，其中包括错误和安全修复。具体相关的代码可在漏洞补丁中查看。

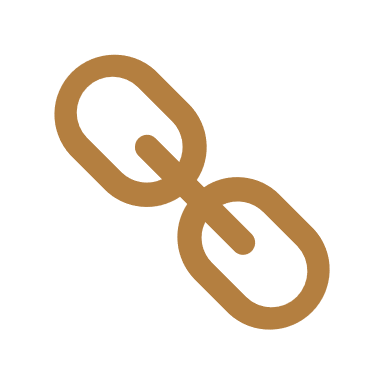
## 漏洞治理

|  |  |  |
| --- | --- | --- |
|  | | |
| 漏洞位置 | bitbucket\_pipeline\_variable 模块中，  根据补丁可以得出漏洞具体位置在plugins/modules/  source\_control/bitbucket/bitbucket\_pipeline\_variable.py  文件中 |
| 漏洞补丁 | <https://github.com/ansible-collections/community.general/pull>  /1635/commits/8de555b5d69debb9bbed877922024385718edd3f  备注: bitbucket\_pipeline\_variable –  隐藏标记为安全的用户敏感信息以防止登录控制台。 |
| 修复版本 | 2.9.18之后 |
| 参考链接 | <https://access.redhat.com/errata/RHSA-2021:2180> |

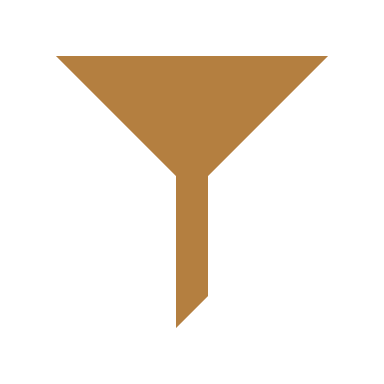
**漏洞5**

**漏洞信息**

* **漏洞编号**: CVE-2021-21686
* **平台**： CVE/NVD
* **链接**： https://nvd.nist.gov/vuln/detail/CVE-2021-21686
* **漏洞披露时间**: 11/04/2021

**在野漏洞报告**：

<https://www.cvedetails.com/cve/CVE-2021-21686>

**漏洞类型**：

*CWE-59 Improper Link Resolution Before File Access ('Link Following')*

*CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')*

**漏洞描述**：

代理到控制器的安全子系统限制了代理进程可以访问Jenkins控制器上的哪些文件。文件路径过滤器不规范化路径，允许操作遵循符号链接到允许的外部目录。

**漏洞危害**

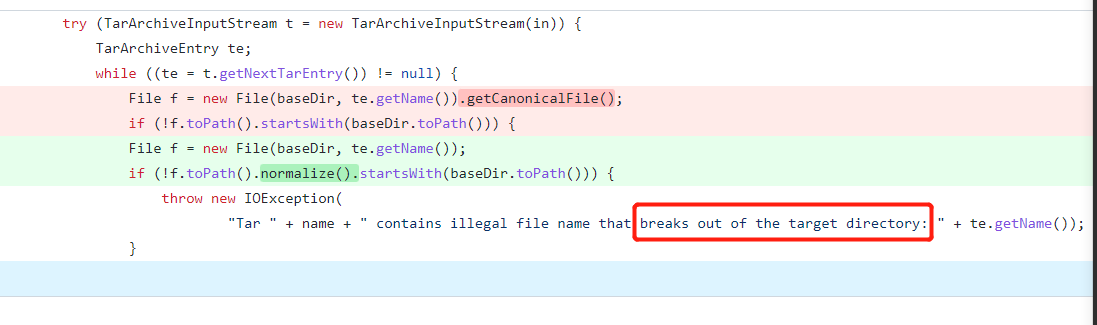
可能允许攻击者读写Jenkins控制器文件系统上的任意文件。

**漏洞评级**：8.1HIGH

**影响版本（网站）**：1.408.1-2.303.2 < 2.318

**漏洞成因**

文件过滤器没有规范路径允许与外部文件创建符号链接。



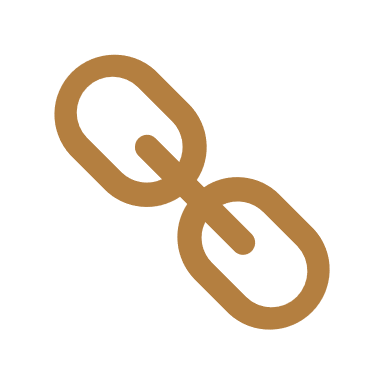
**漏洞治理**

|  |  |  |
| --- | --- | --- |
|  | | |
| 漏洞位置 | core/src/main/java/hudson/FilePath.java 第2840行 |
| 漏洞补丁 | https://github.com/jenkinsci/jenkins/pull/5900/files |
| 修复版本 | 2.303之后 |
| 处置建议 | 建议升级到2.303.2之后，或者直接修改相应位置代码 |
| 参考链接 | <https://www.jenkins.io/security/advisory/2021-11-04/#SECURITY-2455>  <https://github.com/jenkinsci/jenkins/pull/5900/files> |
|  | | |

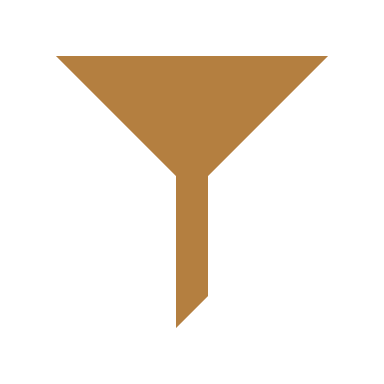
**漏洞6**

**漏洞信息**

* **漏洞编号**: CVE-2021-21687
* **平台**： CVE/NVD
* **链接**： https://nvd.nist.gov/vuln/detail/CVE-2021-21687
* **披露时间**: 11/04/2021

**在野漏洞报告**：

<https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2021-21687>

**漏洞类型**：

[*CWE-862*](http://cwe.mitre.org/data/definitions/862.html) *Missing Authorization*

**漏洞描述**：

Jenkins 2.318 及更早版本、LTS 2.303.2 及更早版本在取消归档 FilePath#untar中的号链接时不检查代理到控制器的访问以创建符号链接。

**漏洞危害**

可能允许攻击者读写Jenkins控制器文件系统上的任意文件。

**漏洞评级**：9.1 Critical

**影响版本（网站）**：1.408.1-2.303.2 2.319之前

**漏洞修复版本**：2.303.3 之后

**漏洞成因**

FilePath#untar 在取消归档符号链接时不检查创建符号链接的权限。

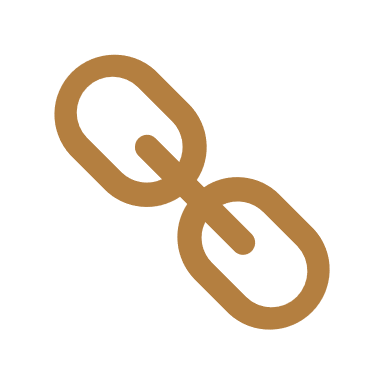
**漏洞治理**

|  |  |
| --- | --- |
|  | |
| 漏洞位置 | core/src/main/java/hudson/FilePath.java 中581行，569行 |
| 漏洞补丁 | https://github.com/jenkinsci/jenkins/pull/5885/files中对于FilePath的修改 |
| 处置建议 | 请升级至2.303.3版本以上 |
| 参考链接 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：  <https://www.jenkins.io/security/advisory/2021-11-04/#SECURITY-2455> |
|  | |

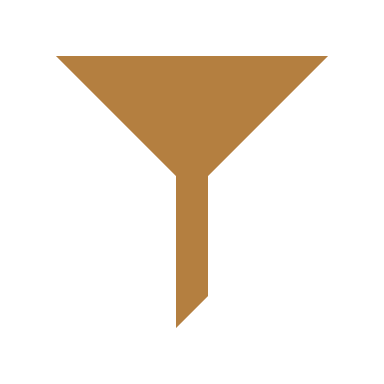
**漏洞7**

**漏洞信息**

* **漏洞编号**: CVE-2021-22147
* **平台**： CVE/NVD
* **链接**： https://nvd.nist.gov/vuln/detail/CVE-2021-22147
* **披露时间**: 03/08/2021

**在野漏洞报告**：

<https://www.suse.com/fr-fr/security/cve/CVE-2021-22147.html>

**漏洞类型**：

[*CWE-862*](http://cwe.mitre.org/data/definitions/862.html) *, CWE-732*

**漏洞描述**：

在 Elasticsearch 中发现了一个缺陷，即文档和字段级安全性未应用于可搜索快照。这可能会导致经过身份验证的用户访问他们未经授权查看的信息。

**漏洞危害**

在Elastic App Search中发现了一个缺陷，即 API 密钥缺少通过备用路由的授权。利用此漏洞，经过身份验证的攻击者可以利用属于更高权限用户的 API 密钥。

**漏洞严重性**：

*NVD: CVSS Version 3.x: 6.5 MEDIUM; CVSS Version 2.0:4.0 MEDIUM*

*SUSE:CVSS Version 3.x: 5.7*

* **影响版本（网站）**：Elasticsearch versions 7.11.0 to 7.13.4

**漏洞修复版本**：7.14.0及以后

**漏洞成因**

在7.14.0 之前的 Elasticsearch 没有对可搜索快照应用文档和字段级别的安全性。这可能会导致经过身份验证的用户获得对他们无权查看的信息的访问权限。

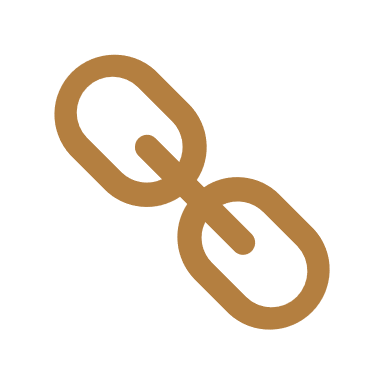
**漏洞治理**

|  |  |
| --- | --- |
|  | |
| 漏洞位置 | <https://github.com/gridgentoo/pulsar/commit/1af8d3fc6bca31c1ca059a2dda80e6d8eb7ae24b#diff-4516062fd37f01febd984641f4312707d17871dc915b6c0be39118ba2325ee03>  函数：testSslBasic() 位置：第45-51行  函数：testSslWithHostnameVerification() 位置：第80-86行  <https://github.com/gridgentoo/pulsar/commit/1af8d3fc6bca31c1ca059a2dda80e6d8eb7ae24b#diff-2c290af7e0a5d1818a605d706015f362e5d9705c74b5d3764038e7f2f278d6e7>  函数：initBeforeClass() 位置：第57-60行  函数：testBulkRetry() 位置：第225-260行 |
| 漏洞补丁 | <https://github.com/gridgentoo/pulsar/commit/1af8d3fc6bca31c1ca059a2dda80e6d8eb7ae24b> |
| 处置建议 | 用户应升级Elasticsearch到版本 7.14.0 |
| 参考链接 | [Elastic Stack 7.14.0 Security Update](https://discuss.elastic.co/t/elastic-stack-7-14-0-security-update/280344): [Elastic Stack 7.14.0 Security Update - Announcements / Security Announcements - Discuss the Elastic Stack](https://discuss.elastic.co/t/elastic-stack-7-14-0-security-update/280344?utm_source=feedly)  Red Hat: [CVE-2021-22147- Red Hat Customer Portal](https://access.redhat.com/security/cve/cve-2021-22147) |
|  | |

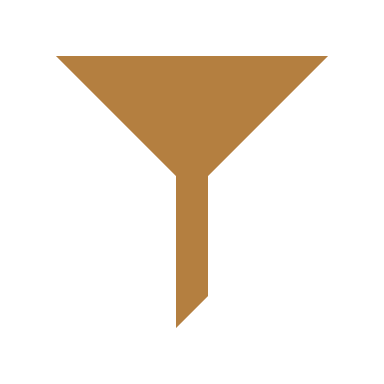
**漏洞8**

**漏洞信息**

* **漏洞编号**: CVE-2021-25640
* **平台**： CVE/NVD
* **链接**： https://nvd.nist.gov/vuln/detail/CVE-2021-25640
* **披露时间**: 06/01/2021

**在野漏洞报告**：

<https://zhuanlan.zhihu.com/p/345902124>

**漏洞类型**：

*CWE-918*

**漏洞描述**：

在Apache Dubbo软件2.6.9到2.7.9版本中，parseURL的使用会导致绕过白名单的检测，从而会引发开放式重定向或者SSRF漏洞。

**漏洞危害**

绕过白名单，可能会引发开放式重定向或者SSRF。

**漏洞评级**：6.1

**影响版本（网站）**：

Dubbo 2.7.0 到 2.7.9版本

Dubbo 2.6.0 到2.6.9版本

Dubbo 所有 2.5.x 版本 (不再被官方维护)

**漏洞修复版本**：Dubbo 2.6.9, 2.7.9

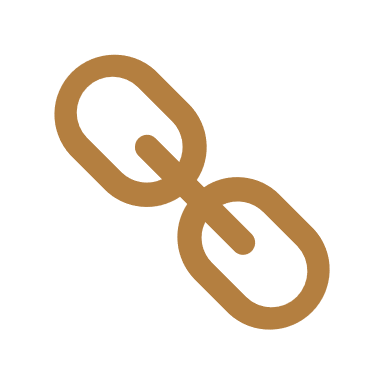
**漏洞治理**

|  |  |
| --- | --- |
|  | |
| 漏洞位置 | dubbo-dubbo-2.7.8\dubbo-common\src\main\java\org\apache\dubbo\common\utils\UrlUtils.java中parseURL函数3 |
| PoC备注 | 该漏洞的解决建议是将软件更新到2.7.10 +或者2.6.9 +，暂时没有发现相关的漏洞poc |
| 漏洞补丁 | <https://github.com/apache/dubbo/commit/b100a6d22b5cf051f76dad2b05aaf88e74e22154> |
| 处置建议 | 根据当前使用的版本将dubbo相应升级到2.7.10+或2.6.9+。  <https://cn.dubbo.apache.org/en/blog/2020/05/18/past-releases/> |
| 参考链接 | <https://zhuanlan.zhihu.com/p/345902124> |
|  | |

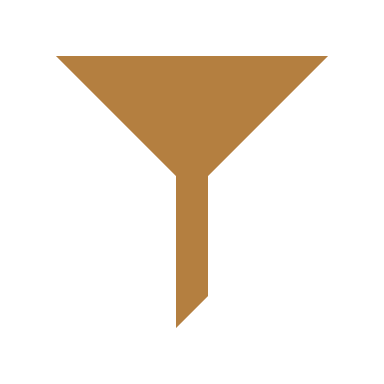
# 漏洞9

## 漏洞信息

* **漏洞编号**: CVE-2021-25641
* **平台**： CVE/NVD
* **链接**： https://nvd.nist.gov/vuln/detail/CVE-2021-25641
* **漏洞披露时间**: 06/01/2021

**在野漏洞报告**：

https://securitylab.github.com/advisories/GHSL-2021-034\_043-apache-dubbo/

**漏洞类型**：

*CWE-502*

**漏洞描述**：

在Apache Dubbo软件2.5.0-2.6.8和2.7.0-2.7.7版本中，dubbo-remoting/dubbo-remoting-api/src/main/java/com/alibaba/dubbo/remoting/transport/CodecSupport.java的getSerialization函数的70-75行存在反序列化问题，会造成远程代码执行。已在2.6.9和2.7.8版本修复。

## 漏洞危害

* **漏洞评级**：9.8 CRITICAL
* **影响版本（网站）**：[ 2.5.0, 2.6.9 ) , [ 2.7.0, 2.7.8 )

## 漏洞成因

虽然hessian2协议通过允许列表限制了反序列化的内容，但是其他反序列化协议没有被这样保护。在RPC请求头指定的序列化协议可以是任意一个以下的协议。

2 -> "hessian2"

3 -> "java"

4 -> "compactedjava"

6 -> "fastjson"

7 -> "nativejava"

8 -> "kryo"

9 -> "fst"

10 -> "native-hessian"

11 -> "avro"

12 -> "protostuff"

16 -> "gson"

21 -> "protobuf-json"

22 -> "protobuf"

25 -> "kryo2"

为了防止攻击者强制执行native Java反序列化，服务器会检查序列化Id，如果攻击者要求执行服务器未配置的反序列化，应用会抛出异常。但是攻击者可以要求运行其余的协议，并且这些协议大多没有受到保护，会导致远程代码执行。

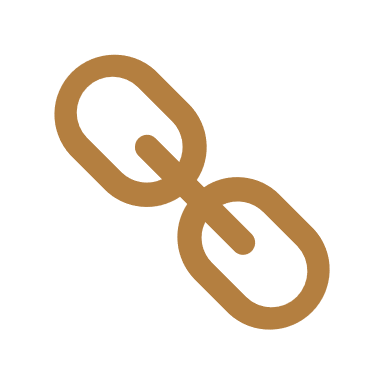
## 漏洞治理

|  |  |  |
| --- | --- | --- |
|  | | |
| 漏洞位置 | dubbo-remoting/dubbo-remoting-api/src/main/java/com/ alibaba/dubbo/remoting/transport/CodecSupport.java  getSerialization函数  70-75行 |
| 漏洞补丁 | [https://github.com/apache/dubbo/commit /077da34addab54d9718710f6848669c4f0d701f1](https://github.com/apache/dubbo/commit%20/077da34addab54d9718710f6848669c4f0d701f1) |
| 漏洞Poc | <https://checkmarx.com/blog/the-0xdabb-of-doom-cve-2021-25641/>  [备注] 文章对应的PoC代码在github仓库:  <https://github.com/Dor-Tumarkin/CVE-2021-25641-Proof-of-Concept> |
| 处置建议 | 建议1：2.6.9和2.7.8版本已修复该漏洞，建议升级至2.6.9或2.7.8版本。  建议2：利用阿里云安全组功能设置Apache Dubbo 相关端口仅对可信地址开放。 |
|  | | |

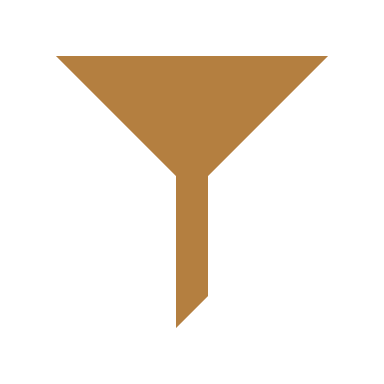
**漏洞10**

**漏洞信息**

* **漏洞编号**: CVE-2021-30179
* **平台**： CVE/NVD
* **链接**： <https://nvd.nist.gov/vuln/detail/CVE-2021-30179>
* **漏洞披露时间**: 06/01/2021

**在野漏洞报告**：

https://securitylab.github.com/advisories/GHSL-2021-034\_043-apache-dubbo/

**漏洞类型**：

*CWE-502 网络远程攻击*

**漏洞描述**：

在CVE-2021-30179中，Apache Dubbo Generic filter过滤不佳。攻击者可以构造恶意请求，调用恶意方法导致远程代码执行。

**漏洞危害**

**漏洞评级**：9.8 HIGH

**影响版本（网站）**：Dubbo 2.7.0 到 2.7.9版本

**漏洞成因**

Apache Dubbo默认支持对提供者接口所暴露的任意方法的调用，而这些调用由GenericFilter处理，它将找到调用的第一个参数中指定的服务和方法，并使用Java Reflection API来进行最终调用。$invoke或$invokeAsync方法的签名是Ljava/lang/String;[Ljava/lang/String;[Ljava/lang/Object；其中第一个参数是要调用的方法的名称，第二个参数是包含被调用方法的参数类型的数组，第三个参数是包含实际调用参数的数组。

Apache Dubbo在处理泛类引用时，提供了多种通过反序列化方式得到对象再生成pojo对象的选择。在进行反序列化过程中没有做好防护，轻易相信用户提供的数据，直接将其进行反序列化操作，导致一些恶意对象的实例化以及相对应Gadget的触发，从而造成RCE。

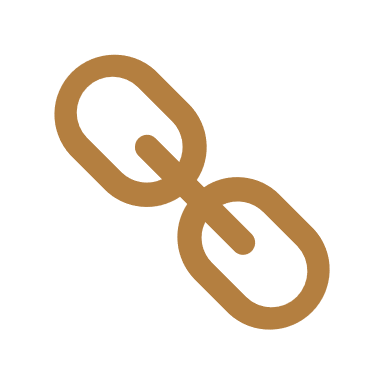
**漏洞治理**

|  |  |  |
| --- | --- | --- |
|  | | |
| 漏洞位置 | 参考链接: <https://cloud.tencent.com/developer/article/1865614>  文中0x03 漏洞分析部分详细展示了该漏洞的位置。 |
| 漏洞补丁 | N/A |
| 修复版本 | 2.7.10 |
| 处置建议 | 1. 升级 Apache Dubbo 至最新版本  2、设置 Apache Dubbo 相关端口仅对可信地址开放。 |
| 漏洞PoC | 链接: <https://cloud.tencent.com/developer/article/1865563> |

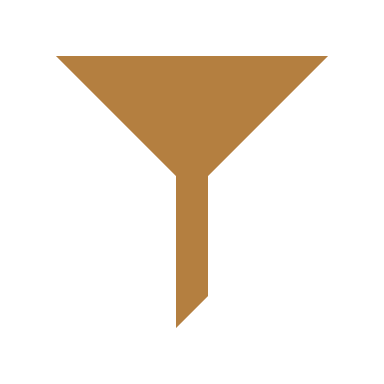
**漏洞11**

**漏洞信息**

* **漏洞编号**: CVE-2021-30180
* **平台**： CVE/NVD
* **链接**： <https://nvd.nist.gov/vuln/detail/CVE-2021-30180>
* **漏洞披露时间**: 06/01/2021

**在野漏洞报告**：

https://securitylab.github.com/advisories/GHSL-2021-034\_043-apache-dubbo/

**漏洞类型**：

*CWE-444*

**漏洞描述**：

Apache Dubbo 2.7.9 之前的版本支持标签路由，这将使客户能够将请求路由到正确的服务器。客户在发出请求时使用这些规则来查找正确的终结点。在解析这些 YAML 规则时，Dubbo 客户可以启用调用任意构造函数。

**漏洞危害**

**漏洞评级**：9.8 CRITICAL 6.8 MEDIUM

**影响版本（网站）**：dubbo: [2.7.0, 2.7.10)

**漏洞成因**

Apache Dubbo多处使用了yaml.load，攻击者在控制如ZooKeeper注册中心后可上传恶意配置文件从而造成了Yaml反序列化漏洞。

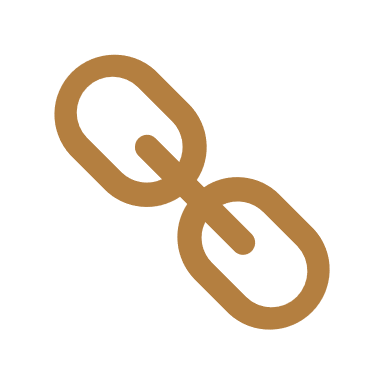
**漏洞治理**

|  |  |  |
| --- | --- | --- |
|  | | |
| 漏洞位置 | dubbo/TagRuleParser.java at f4b225eb3a5acdf7c9064763f522ea0b86421c8d · apache/dubbo (github.com) |
| 漏洞补丁 | Use safeConstructor instead of constructor when parsing yaml by kevinw66 · Pull Request #7437 · apache/dubbo (github.com) |
| 修复版本 | 2.7.10-2.7.15 |
| 处置建议 | 升级至2.7.10及以上版本 |
| 参考链接 | [【安全通报】Apache Dubbo 多个预认证 RCE 漏洞（CVE-2021-25641等）|NOSEC安全讯息平台 - 白帽汇安全研究院](https://www.nosec.org/home/detail/4778.html)  [Apache Dubbo漏洞跟进研究 - 唐小风 - 博客园 (cnblogs.com)](https://www.cnblogs.com/suyu7/p/14928710.html)  [Apache Dubbo相关漏洞复现 | CN-SEC 中文网](https://cn-sec.com/archives/406069.html) |
|  | | |

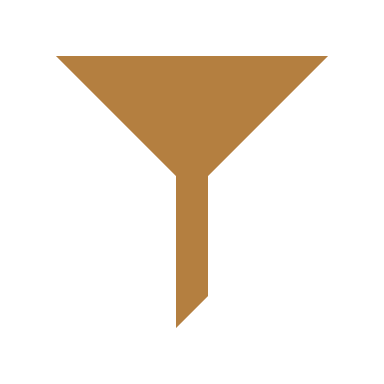
**漏洞12**

**漏洞信息**

* **漏洞编号**: CVE-2021-30181
* **平台**： CVE/NVD
* **链接**： https://nvd.nist.gov/vuln/detail/CVE-2021-30181
* **漏洞披露时间**: 06/01/2021

**在野漏洞报告**：

https://securitylab.github.com/advisories/GHSL-2021-034\_043-apache-dubbo/

**漏洞类型**：

*NVD-CWE-noinfo*

**漏洞危害**

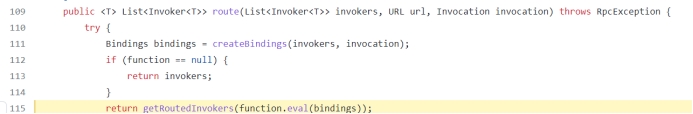
**漏洞评级**：9.8

**漏洞成因**

Apache Dubbo支持脚本路由，这将使客户能够将请求路由到正确的服务器。 这些规则被加载到配置中心（例如：ZooKeeper、Nacos等）并由客户在发出请求时检索以找到正确的端点。

在解析这些规则时，Dubbo客户将使用JRE ScriptEngineManager加载一个ScriptEngine并运行脚本提供的规则，该规则默认允许执行任意Java代码。

如果攻击者访问了配置中心（ZooKeeper、Nacos等）并设置了恶意的Script规则文件，就可以在消费者接受到规则时 ，进行攻击。



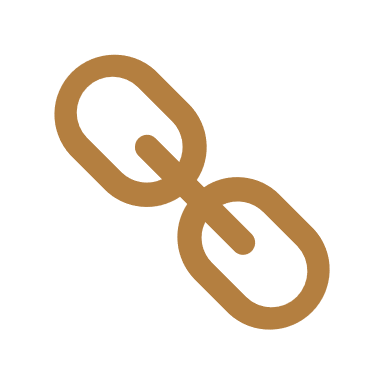
**漏洞治理**

|  |  |  |
| --- | --- | --- |
|  | | |
| 漏洞位置 | <https://github.com/apache/dubbo/blob/f4b225eb3a5acdf>  7c9064763f522ea0b86421c8d/dubbo-cluster/src/main/java/org/apache/dubbo/rpc/cluster  /router/script/ScriptRouter.java#L115 |
| 漏洞补丁 | Use java box to prevent malicious code. by horizonzy · Pull Request #7428 · apache/dubbo (github.com) |
| 修复版本 | 2.303之后 |
| 处置建议 | 升级至2.7.10及以上版本  修改代码补丁，参考  Use java box to prevent malicious code. by horizonzy · Pull Request #7428 · apache/dubbo (github.com) |
| 参考链接 | https://nvd.nist.gov/vuln/detail/CVE-2021-30181  https://securitylab.github.com/advisories/GHSL-2021-034\_043-apache-dubbo/Use java box to prevent malicious code. by horizonzy · Pull Request #7428 · apache/dubbo (github.com) |
|  | | |

**漏洞13**

**漏洞信息**

* **漏洞编号**: CVE-2021-30639
* **平台**： CVE/NVD
* **链接**： <https://nvd.nist.gov/vuln/detail/CVE-2021-30639>
* **漏洞披露时间**: 07/26/2022

**在野漏洞报告**：

<https://cloud.tencent.com/announce/detail/1550>

**漏洞描述**：

Apache Tomcat 中的漏洞允许攻击者远程发起拒绝服务攻击。这个错误是作为改进非阻塞 I/O 期间错误处理的一部分引入，意味着与 Request 对象关联的错误标志不会在请求之间重置。这意味着一旦发生非阻塞 I/O 错误，该请求对象处理的所有未来请求都将失败。用户能够触发非阻塞 I/O 错误，例如通过断开连接，从而产生触发 DoS 的可能性。不使用非阻塞 I/O 的应用程序不会暴露于此漏洞。

**漏洞危害**

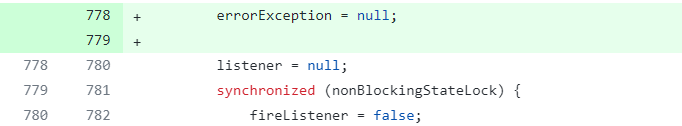
**漏洞评级**：7.5HIGH

**影响版本（网站）**：Tomcat:<8.5.64;<9.0.44;10.0.3;<10.0.4;

epolicy\_orchestrator:2.0-5.10.0;big\_data\_spatial\_and\_graph:2.0-23.1

**漏洞成因**

未能回收新添加的 errorException 对象意味着一旦aysnc 读取发生错误，所有后续异步读取都将失败。



这里原来没有及时吧errorException置空，导致异步阻塞。

漏洞类型: CWE-755 Improper Handling of Exceptional Conditions

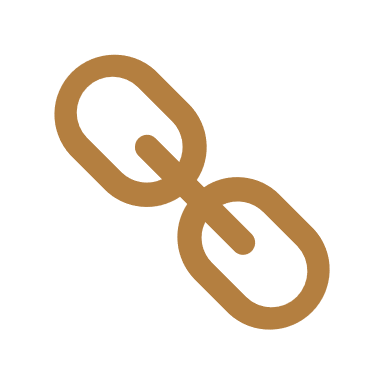
**漏洞治理**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
| 漏洞位置 | | 无 | | |
| 漏洞补丁 | https://github.com/apache/tomcat/commit/b59099e4ca501a039510334ebe1024971cd6f959 | | |
| 修复版本 | | 2.303之后 | | |
| 处置建议 | | 官方已发布漏洞修复版本，请评估业务是否受影响后，酌情升级至上述安全版本 | | |
| 参考链接 | | <https://bz.apache.org/bugzilla/show_bug.cgi?id=65203>  <https://tomcat.apache.org/security-10.html> | | |
|  | | |

**漏洞14**

**漏洞信息**

* **漏洞编号**: CVE-2021-43297
* **平台**： CVE/NVD
* **链接**： https://nvd.nist.gov/vuln/detail/CVE-2021-43297
* **漏洞披露时间**: 01/10/2022

**在野漏洞报告**：

<https://cert.360.cn/warning/detail?id=413132b068d5e062e3059adc758d3500>

这是360网络安全响应中心给出的报告，较为全面，此外还有一篇报告

<https://www.freebuf.com/articles/network/320134.html> ，对漏洞分析地比较透彻。

**漏洞危害**

**漏洞评级**：9.8

**影响版本（网站）**：Apache Dubbo 2.6.0 - 2.6.12 ； 2.7.0 - 2.7.15 ； 3.0.0 -3.0.5

**漏洞成因**

Dubbo Hessian-Lite 3.2.11及之前版本中存在潜在RCE攻击风险。Hessian-Lite在遇到序列化异常时会输出相关信息，这可能导致触发某些恶意定制的Bean的toString方法，从而引发RCE攻击。这个CVE主要还是从Hessian2Input.except()->obj.toString触发的。

下面有几种触发方法：

第一种：JsonObject.toString

dubbo<=2.7.3时，由于其自带fastjson<=1.2.46版本，所以可以用JsonObject包裹一个TemplatesImpl对象，该TemplatesImpl的\_bytecodes属性携带恶意字节码，在恶意字节码实例化的过程中实现RCE，但是有版本限制

第二种：ReadOnlyBinding.toString

其实是[XBean调用链](https://github.com/threedr3am/learnjavabug/blob/master/dubbo/src/main/java/com/threedr3am/bug/dubbo/XBeanPoc.java" \t "https://www.cnblogs.com/bitterz/p/_blank)的截断，截断后的调用链如下，其实就是利用其toString方法往下调用时会用到NamingManager，在NamingManager中会去指定地址下载恶意class文件，并实例化，最终造成RCE。

<https://github.com/threedr3am/learnjavabug/blob/master/dubbo/src/main/java/com/threedr3am/bug/dubbo/XBeanPoc.java>

截断后的调用链

at java.lang.Class.newInstance(Class.java:442)

at javax.naming.spi.NamingManager.getObjectFactoryFromReference(NamingManager.java:163)

at javax.naming.spi.NamingManager.getObjectInstance(NamingManager.java:319)

at org.apache.xbean.naming.context.ContextUtil.resolve(ContextUtil.java:73)

at org.apache.xbean.naming.context.ContextUtil$ReadOnlyBinding.getObject(ContextUtil.java:204)

at javax.naming.Binding.toString(Binding.java:192)

I/O 的应用程序不会暴露于此漏洞。

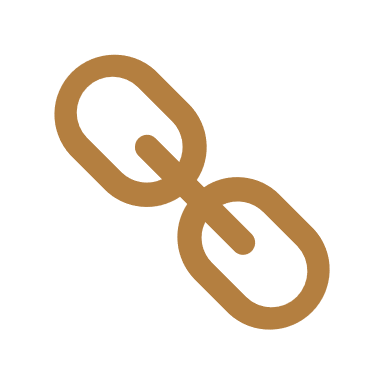
**漏洞治理**

|  |  |  |
| --- | --- | --- |
|  | | |
| 漏洞位置 | src/main/java/com/alibaba/com/caucho/hessian/io/Hessian2Input.java第3566行；src/main/java/com/alibaba/com/caucho/hessian/io/JavaDeserializer.java第171行 |
| 漏洞poc | <https://github.com/bitterzzZZ/CVE-2021-43297-POC> |
| 修复版本 | 无 |
| 处置建议 | 无 |
| 参考链接 | 无 |
|  | | |

**漏洞15**

**漏洞信息**

* **漏洞编号**: CVE-2021-44224
* **平台**： CVE/NVD
* **链接**： [https://nvd.nist.gov/vuln/detail/CVE-2021-44224](https://nvd.nist.gov/vuln/detail/CVE-2021-30639)
* **漏洞披露时间**: 12/20/2021

**在野漏洞报告**：

<https://cert.360.cn/warning/detail?id=9eddce1b5120cc0b0ec423f17aaf2940>

**漏洞危害**

**漏洞评级**：8.2

**影响版本（网站）**：

apache:http\_server 2.4.7-2.4.52

tenable:tenable.sc 5.14.0-5.20.0； 5.16.0-202201.1

apple:macos 11.0-11.6.6； 12.0.0-12.4

**漏洞成因**

如果httpd 配置作为转发代理（ProxyRequests on） ，可允许攻击者通过精心构造的 URI ，导致崩溃（空指针取消引用），或者如果httpd的配置为混合转发和反向代理声明，可以允许攻击者将请求发送到声明的 Unix 域套接字端点，造成服务器端请求伪造。

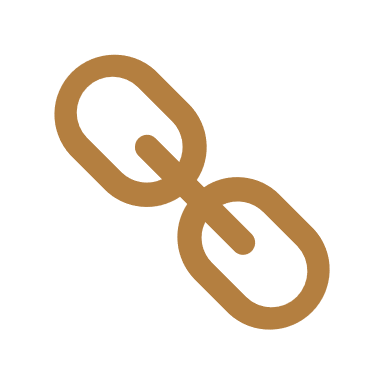
**漏洞治理**

|  |  |
| --- | --- |
|  | |
| 漏洞位置 | 无 |
| 漏洞补丁 | https://www.h3c.com/cn/d\_202112/1519672\_30003\_0.htm |
| 参考链接 | https://bugzilla.redhat.com/show\_bug.cgi?id=2034672 |

**漏洞16**

**漏洞信息**

* **漏洞编号**: CVE-2021-44790
* **平台**： CVE/NVD
* **链接**： <https://nvd.nist.gov/vuln/detail/CVE-2021-44790>
* **漏洞披露时间**: 12/20/2021

**在野漏洞报告**：

<https://www.zerodayinitiative.com/blog/2022/1/25/cve-2021-44790-code-execution-on-apache-via-an-integer-underflow>

**漏洞描述**：

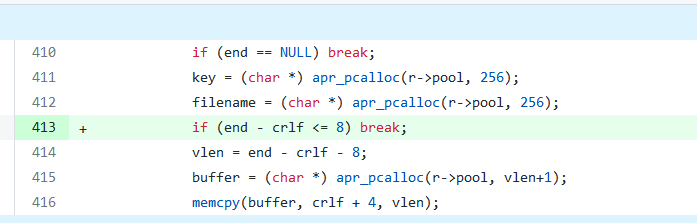
精心设计的请求主体可能会导致 mod\_lua 多部分解析器（从 Lua 脚本调用 r:parsebody()）中的缓冲区溢出。 Apache httpd 团队并不清楚该漏洞的利用，尽管这是有可能被制作的。此漏洞会影响 Apache HTTP Server 2.4.51 及更早版本。

**漏洞危害**

**漏洞评级**：9.8

**影响版本（网站）**：Apache http\_server: 2.4.52之前的版本

在2.4.52版本之前都没有添加对于字符串长度的检验，会导致缓存区溢出攻击，在2.4.52版本加入了以下的判断，这样避免了长度溢出：



Fedoraproject fedora 34 - 36版本

Debian debian\_linux 10.0 , 11.0

Tenable tenable.sc 5.16.0 - 5.20.0

Netapp cloud\_backup

Oracle communications\_operations\_monitor 4.3 , 4.4 , 5.0

Oracle communications\_element\_manager 9.0之前的版本

Oracle communications\_session\_report\_manager 9.0之前的版本

Oracle communications\_session\_route\_manager 9.0之前的版本

Oracle http\_server 12.2.1.3.0 , 12.2.1.4.0

Oracle instantis\_enterprisetrack 17.1 - 17.3

Oracle zfs\_storage\_appliance\_kit 8.8

Apple mac\_os\_x 10.15.7 security\_update\_2020-001

Apple mac\_os\_x 10.15.7 security\_update\_2021-001 - 2021-008

Apple mac\_os\_x 10.15.7 security\_update\_2022-001 - 2022-003

Apple macos 10.15.7之前的版本

Apple macos 11.0 - 11.6.6

Apple macos 12.0 - 12.4

漏洞修复的组件版本: Apache http\_server: 2.4.52

**漏洞成因**

精心设计的请求主体可能会导致 mod\_lua 多部分解析器中的缓冲区溢出，这可能会导致代码在安全进程的上下文中执行。Apache httpd 的 mod\_lua 模块中出现了一个整数溢出漏洞。该漏洞是由于模块的多部分解析器中的请求主体验证不正确，通过 Lua 脚本中的 r:parsebody() 函数调用。未经身份验证的远程攻击者可以通过向目标服务器发送精心设计的请求来利用此漏洞。成功利用可能导致在服务器进程的安全上下文下远程执行代码，而不成功的攻击可能导致拒绝服务条件。

**漏洞治理**

|  |  |
| --- | --- |
|  | |
| 漏洞位置 | <https://www.venustech.com.cn/new_type/aqldfx/20220120/23400.html>  根据漏洞公告，可知漏洞存在于mod\_lua模块中，lua脚本调用了r:parsebody()函数发生了缓冲区溢出。结合patch信息，直接定位到req\_parsebody函数内 |
| 漏洞补丁 | <https://github.com/apache/httpd/commit/07b9768cef6a224d256358c404c6ed5622d8acce>  备注: 该漏洞在Apache HTTP Server 2.4.52中进行了修复。在内存申请之前，增加了对长度的合法性校验。 |
| 处置建议 | <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BFSWOH4X77CV7AH7C4RMHUBDWKQDL4YH/> |
| 参考链接 | <https://www.venustech.com.cn/new_type/aqldfx/20220120/23400.html> |

# 总结

**Vulnerability Detection Summary**

**检测结果显示，您的漏洞亟需处理，请尽快将其修复。**

**本次漏洞检测报告完毕，感谢您对本服务的使用和支持。**

**2023/04/04**