

MapReduce 服务

服务公告

文档版本 01
发布日期 2025-02-18



版权所有 © 华为云计算技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

1 漏洞公告	1
1.1 Apache Log4j2 远程代码执行漏洞（CVE-2021-44228）公告	1
1.2 Apache Log4j2 远程代码执行漏洞（CVE-2021-44228）修复指导	2
1.3 MRS Fastjson 漏洞修复指导	6
1.3.1 简介	6
1.3.2 影响范围	7
1.3.3 修复 Manager Web	7
1.3.4 修复 Manager Controller	8
1.3.5 修复 Manager nodeagent	9
1.3.6 修复 Kafka	9
1.3.7 修复 Flink	10
2 版本支持公告	12
2.1 MRS 集群版本生命周期	12

1 漏洞公告

1.1 Apache Log4j2 远程代码执行漏洞 (CVE-2021-44228) 公告

漏洞描述

近日，华为云关注到Apache Log4j2存在一处远程代码执行漏洞（ CVE-2021-44228 ），在引入Apache Log4j2处理日志时，会对用户输入的内容进行一些特殊的处理，攻击者可以构造特殊的请求，触发远程代码执行。目前POC已公开，风险较高。具体漏洞详情，请参见[Apache Log4j2 远程代码执行漏洞 \(CVE-2021-44228 \)](#)。

漏洞影响

在MapReduce服务（简称MRS）中Hive、Flink、Spark、Manager(Tomcat)、Tez、Impala、Ranger、Presto、Oozie、Storm、Loader等组件有使用Apache Log4j2。在默认情况下集群不会对外网开放，如您通过绑定EIP等方式开放了公网访问权限，请确认输入源是否可信，同时建议您根据[漏洞规避方案](#)进行加固。

漏洞规避方案

请根据MRS集群版本，从如下链接中选择相应的漏洞规避方案。

- MRS 3.1.1: [MRS 3.1.1版本Log4j2远程执行漏洞 \(CVE-2021-44228 \) 缓解措施](#)
- MRS 3.1.0: [MRS 3.1.0版本Log4j2远程执行漏洞 \(CVE-2021-44228 \) 缓解措施](#)
- MRS 3.0.5: [MRS 3.0.5版本Log4j2远程执行漏洞 \(CVE-2021-44228 \) 缓解措施](#)
- MRS 3.0.2: [MRS 3.0.2版本Log4j2远程执行漏洞 \(CVE-2021-44228 \) 缓解措施](#)
- MRS 2.1.1: [MRS 2.1.1版本Log4j2远程执行漏洞 \(CVE-2021-44228 \) 缓解措施](#)
- MRS 2.1.0: [MRS 2.1.0版本Log4j2远程执行漏洞 \(CVE-2021-44228 \) 缓解措施](#)
- MRS 1.9.3: [MRS 1.9.3版本Log4j2远程执行漏洞 \(CVE-2021-44228 \) 缓解措施](#)
- MRS 1.9.2: [MRS 1.9.2版本Log4j2远程执行漏洞 \(CVE-2021-44228 \) 缓解措施](#)
- MRS 1.9.0: [MRS 1.9.0版本Log4j2远程执行漏洞 \(CVE-2021-44228 \) 缓解措施](#)

- MRS 1.8.10: [MRS 1.8.10版本Log4j2远程执行漏洞 \(CVE-2021-44228\) 缓解措施](#)
- MRS 1.7.1: [MRS 1.7.1版本Log4j2远程执行漏洞 \(CVE-2021-44228\) 缓解措施](#)

1.2 Apache Log4j2 远程代码执行漏洞 (CVE-2021-44228) 修复指导

本章节指导用户修复log4j2的CVE-2021-44228漏洞。目前有两种方式可以采用如下两种方式修复：

- [现有集群节点安装补丁](#)
- [扩容节点安装补丁](#)

前提条件

- 从OBS路径中下载的补丁工具“MRS_Log4j_Patch.tar.gz”，下载路径：https://mrs-container1-patch-cn-south-1.obs.cn-south-1.myhuaweicloud.com/MRS_Common_Script/MRS_Log4j_Patch.tar.gz。
- 确认集群主OMS节点：

📖 说明

OMS节点一般为Master1和Master2节点，主OMS节点判断方法，执行以下命令，返回结果为active的节点为主OMS节点，返回结果为standby的节点为备OMS节点：

3.x之前版本：

```
sh /opt/Bigdata/*/workspace0/ha/module/hacom/script/get_harole.sh
```

3.x及之后版本：

```
sh /opt/Bigdata/om-server*/OMS/workspace0/ha/module/hacom/script/get_harole.sh
```

现有集群节点安装补丁

步骤1 将“MRS_Log4j_Patch.tar.gz”上传至主OMS节点的“/home/omm”目录下。具体可参考[如何上传本地文件到集群内节点？](#)。

步骤2 使用root用户登录主OMS节点，修改补丁工具相应权限，切到omm用户下，并解压补丁工具至当前目录。

```
chown omm:wheel -R /home/omm/MRS_Log4j_Patch.tar.gz
```

```
su - omm
```

```
cd /home/omm
```

```
tar -zxf MRS_Log4j_Patch.tar.gz
```

步骤3 在“/home/omm/MRS_Log4j_Patch/bin/ips.ini”文件中配置需要打补丁的节点IP（当前集群所有节点IP）。

📖 说明

每行配置一个IP，中间不能有空行。

步骤4 执行脚本安装补丁。

```
cd /home/omm/MRS_Log4j_Patch/bin
```

```
nohup sh install.sh upgrade &
```

通过`tail -f nohup.out`可查看执行情况（打印“upgrade patch success.”表示执行完成）。

步骤5 登录Manager页面，重启受影响的组件，受影响组件请参考[受影响组件列表](#)。建议业务低峰期时执行重启操作。

步骤6 （可选）如果要新下载的客户端安装上补丁，需要先为部件包安装补丁，可执行如下命令：

```
su - omm
```

```
cd /home/omm/MRS_Log4j_Patch/bin
```

```
nohup sh install.sh upgrade_package &
```

通过`tail -f nohup.out`查看执行情况，打印“upgrade_package patch success.”表示执行完成。

执行完之后，重新下载的客户端就已经是安装补丁的客户端。

⚠ 注意

- 该步骤耗时比较长，且执行完之后不需要重启组件。
- 补丁安装完成后，不能删除补丁目录相关文件，否则会响补丁的卸载功能。

----结束

扩容节点安装补丁

步骤1 扩容操作时关闭“启动组件”开关。

The screenshot shows a configuration window for expanding nodes. The title is '扩容' (Expansion). It lists current node specifications: 4 vCPUs 32 GB | m6.xlarge.8, 480 GB 高IO (High IO) system disk, 600 GB 高IO * 1 (High IO * 1) data disk, and 3 current nodes. A red box highlights the '启动组件' (Start Component) toggle switch, which is currently turned off. Other settings include a purchase duration of 31 days 7 hours 59 minutes, a configuration fee of ¥1085.40, and an expansion node count of 1. A red message at the bottom states: '您当前的可用配额最多可以创建2个节点，申请扩大配额' (Your current available quota can create up to 2 nodes, apply for expansion). At the bottom are '确定' (Confirm) and '取消' (Cancel) buttons.

步骤2 将“MRS_Log4j_Patch.tar.gz”上传至主OMS节点的“/home/omm”目录下。具体可参考[如何上传本地文件到集群内节点？](#)。

步骤3 使用root用户登录主OMS节点，修改补丁工具相应权限，切换到omm用户下，并解压补丁工具至当前目录。

```
chown omm:wheel -R /home/omm/MRS_Log4j_Patch.tar.gz
```

```
su - omm
```

```
cd /home/omm
```

```
tar -zxf MRS_Log4j_Patch.tar.gz
```

步骤4 在“/home/omm/MRS_Log4j_Patch/bin/ips.ini”文件中配置需要打补丁的节点IP（当前集群扩容节点IP）。

📖 说明

每行配置一个IP，中间不能有空行。

步骤5 执行脚本安装补丁。

```
cd /home/omm/MRS_Log4j_Patch/bin
```

```
nohup sh install.sh upgrade &
```

通过tail -f nohup.out可查看执行情况，打印“upgrade patch success.”表示执行完成。

步骤6 登录Manager页面，启动新扩容节点上的实例。

----结束

补丁卸载方法

步骤1 使用root用户登录主OMS节点，执行如下命令，卸载脚本：

```
su - omm
```

```
cd /home/omm/MRS_Log4j_Patch/bin
```

```
nohup sh install.sh rollback &
```

通过tail -f nohup.out可查看执行情况，打印“rollback patch success.”表示执行完成。

步骤2 登录Manager页面，重启受影响的组件，受影响组件请参考[受影响组件列表](#)。建议业务低峰期时执行重启操作。

步骤3 如果安装补丁时执行了[现有集群节点安装补丁的步骤6](#)，且希望回退部件包中的修改，可在[步骤2](#)执行完之后执行如下操作：

使用root用户登录主OMS节点，执行如下命令：

```
su - omm
```

```
cd /home/omm/MRS_Log4j_Patch/bin
```

```
nohup sh install.sh rollback_package &
```

通过`tail -f nohup.out`查看执行情况（打印“rollback_package patch success.”表示执行完成）。

----结束

ECS 重置密码插件升级（可选）

华为云ECS服务提供了一键式重置密码功能，弹性云服务器的密码丢失或过期时，可使用该功能进行一键式重置密码。重置密码插件为ECS内部运行的客户端进程，不对外提供任何网络服务，重置密码插件CloudResetPwdUpdateAgent使用了Apache Log4j2组件，经华为云安全实验室分析验证，ECS重置密码插件无可利用条件，无安全风险。

如果用户需要升级该插件中的Log4j2版本，可通过下面的步骤升级插件：

步骤1 将“MRS_Log4j_Patch.tar.gz”上传至主OMS节点的“/home/omm”目录下。具体可参考[如何上传本地文件到集群内节点？](#)。

步骤2 使用root用户登录主OMS节点，修改补丁工具相应权限，切到omm用户下，并解压补丁工具至当前目录。

```
chown omm:wheel -R /home/omm/MRS_Log4j_Patch.tar.gz
```

```
su - omm
```

```
cd /home/omm
```

```
tar -zxf MRS_Log4j_Patch.tar.gz
```

步骤3 在“/home/omm/MRS_Log4j_Patch/bin/ips.ini”文件中配置需要打补丁的节点IP（当前集群所有节点IP）。

📖 说明

每行配置一个IP，中间不能有空行。

步骤4 根据节点登录方式执行以下步骤：

- **密码登录**

执行以下命令：

```
nohup sh install.sh upgrade_resetpwdagent passwd:登录密码 &
```

例如密码为xyz123，则命令为：

```
nohup sh install.sh upgrade_resetpwdagent passwd:xyz123 &
```

通过`tail -f nohup.out`查看执行情况，打印“upgrade_resetpwdagent patch success.”表示执行完成。

- **密钥登录**

a. 将root用户对应的私钥文件上传到“/home/omm/MRS_Log4j_Patch/bin”目录下，保证文件的属组为root:root，执行命令：

```
chown root:root /home/omm/MRS_Log4j_Patch/bin/密钥文件
```

```
chmod 644 /home/omm/MRS_Log4j_Patch/bin/密钥文件
```

b. 执行以下命令

```
su - omm
```

```
cd /home/omm/MRS_Log4j_Patch/bin
```

```
nohup sh install.sh upgrade_resetpwdagent privatekey:私钥文件路径 &
```

例如私钥文件路径为 ‘/home/omm/MRS_Log4j_Patch/bin/abc.pem’，则执行命令为：

```
nohup sh install.sh upgrade_resetpwdagent privatekey:/home/omm/MRS_Log4j_Patch/bin/abc.pem &
```

通过tail -f nohup.out查看执行情况，打印“upgrade_resetpwdagent patch success.”表示执行完成。

---结束

受影响组件列表

MRS集群版本	受影响组件
MRS 3.1.1	Hive、Oozie、Flink、Ranger、Tez
MRS 3.1.0	Hive、Flink、Spark、Tez、Impala、Ranger、Presto、Oozie
MRS 3.0.5	Hive、Flink、Spark、Tez、Impala、Ranger、Presto、Oozie、Storm、Loader
MRS 3.0.2	Hive、Flink、Spark、Tez、Ranger、Oozie、Storm、Loader
MRS 2.1.1	Hive、Tez、Storm、Loader、Impala、Presto
MRS 2.1.0	Loader、Hive、Storm、Presto、Impala、Tez、Spark、HBase
MRS 1.9.3	Loader、Hive、Tez、Spark、Flink
MRS 1.9.2	Loader、Hive、Tez、Spark、Flink、Impala
MRS 1.9.0	Loader、Hive、Spark、Flink
MRS 1.8.10	Loader、Storm
MRS 1.7.1	Loader、Storm

1.3 MRS Fastjson 漏洞修复指导

1.3.1 简介

问题描述

Fastjson披露存在一处反序列化远程代码执行漏洞，漏洞影响所有1.2.80及以下版本，成功利用漏洞可绕过autoType限制，实现远程任意执行代码。

影响风险

存在漏洞的业务被攻击时，将可能导致攻击者远程在业务平台中执行任意代码。

预防与建议

在产品未发布对应解决方案前，建议您参考以下的相关预防措施。

1. 加固物理设备安全边界，防止外网直接访问及攻击内网管理平面。
2. 排查平台各组件节点是否使用默认密码，如果有，建议修改新密码。
3. 加强环境管理面账户密码管控，确保不泄露不扩散。
4. 部分安全厂商已经提供了针对该漏洞的预防措施，您可联系对应的安全厂商，通过在安全设备上设置拦截规则来预防此类攻击。

1.3.2 影响范围

涉及版本

MRS 3.x

涉及模块

- 管理面：不涉及该漏洞
- 租户面：Manager（Web+Controller+nodeagent）、Kafka、Flink

📖 说明

- MRS 3.1.0.x执行以下章节：
 - [修复Manager Web](#)
 - [修复Manager Controller](#)
 - [修复Manager nodeagent](#)
- MRS 3.1.2.x执行章节：
 - [修复Manager Web](#)
 - [修复Manager Controller](#)
 - [修复Manager nodeagent](#)
 - [修复Kafka](#)
 - [修复Flink](#)

1.3.3 修复 Manager Web

前提条件

已获取FusionInsight Manager登录地址及admin账号。

操作步骤

步骤1 使用omm用户登录到主OMS节点，备份“\$OM_TOMCAT_HOME/bin/catalina.sh”文件。

```
cp $OM_TOMCAT_HOME/bin/catalina.sh /tmp
```

步骤2 执行命令vi \$OM_TOMCAT_HOME/bin/catalina.sh，找到“Execute The Requested Command”所在行，在该行上面添加一行新内容：

```
JAVA_OPTS="$JAVA_OPTS -Dfastjson.parser.safeMode=true"
```




步骤2 单击“保存”，配置保存完成后。在Kafka实例页签勾选所有“KafkaUI”实例，选择“更多 > 重启实例”。



步骤3 使用omm用户登录任意KafkaUI实例节点，查看进程：

```
ps -ef | grep KafkaUI
```

如果包含参数“-Dfastjson.parser.safeMode=true”，说明漏洞问题已经规避，如下所示：

```
omm@10.10.10.10:~$ ps -ef | grep KafkaUI
```

----结束

1.3.7 修复 Flink

前提条件

已获取FusionInsight Manager登录地址及admin账号。

操作步骤

步骤1 登录FusionInsight Manager页面，选择“集群 > 服务 > Flink > 配置 > 全部配置”，搜索参数“FLINK_SERVER_GC_OPTS”，在该参数值中添加“-Dfastjson.parser.safeMode=true”（注意与前参数有空格），如下所示：

例如原参数值为：“xxx”，则修改后的参数值为：“xxx -Dfastjson.parser.safeMode=true”。



步骤2 单击“保存”，配置保存完成后。在Flink实例页签勾选所有“FlinkServer”实例，选择“更多 > 重启实例”。



步骤3 使用omm用户登录任意FlinkServe实例节点，查看进程：

ps -ef | grep FlinkServer

如果包含参数“-Dfastjson.parser.safeMode=true”，说明漏洞问题已经规避，如下所示：



----结束

2 版本支持公告

2.1 MRS 集群版本生命周期

版本号说明

MRS当前提供两种版本集群的创建：普通版和LTS版。

- **MRS普通版集群版本号**：格式为**a.b.c.d**，其中**a.b**为大版本号，**c**为小版本号，**d**为补丁版本，例如 MRS 3.1.5.1。
 - a：代表了版本有较大的变动。
 - b：代表了版本有一些组件的变动。
 - c：代表了小版本的变动，可以向前兼容。
 - d：代表了补丁版本，用于问题修复。

图 2-1 MRS 普通版集群版本号



- **MRS LTS版集群版本号**：格式为**a.b.c-LTS.d**，其中**a.b**为大版本号，**c**为小版本号，**d**为补丁版本，例如 MRS 3.2.0-LTS.1。
 - a：代表了版本有较大的变动。
 - b：代表了版本有一些组件的变动。
 - c：代表了小版本的变动，可以向前兼容。
 - d：代表了补丁版本，用于问题修复。

图 2-2 MRS LTS 版集群版本号



版本支持情况

- **集群创建**
MRS同一版本类型下最多同时支持两个大版本的创建。
例如支持创建MRS 3.3.0-LTS、MRS 3.2.0-LTS版本集群，当MRS 3.3.0-LTS发布商用后，之前较早的版本（如MRS 3.1.2-LTS）默认将不在控制台上提供创建入口。对存量用户使用的MRS 3.1.2-LTS版本集群不影响。
- **集群版本升级**
MRS LTS版本集群支持大版本升级的演进路线，默认情况下只支持跨一个版本的升级，如MRS 3.1.2-LTS支持升级到MRS 3.2.0-LTS，MRS 3.2.0-LTS支持升级到MRS 3.3.0-LTS。
- **集群补丁升级**
现网存量运行的MRS集群，如果有大数据组件社区重大问题或者漏洞，MRS将提供对集群打补丁能力，详情请参见[MRS集群补丁说明](#)。

版本约束

- 集群升级到新版本后，不支持回退到老版本。
- 普通版集群不支持升级。

版本发布周期/版本生命周期

表 2-1 生命周期常用术语

术语	定义
停止销售 (EOM)	指停止云服务版本的部署，现网中不再部署该云服务版本。
停止全面支持 (EOFS)	指定云服务版本停止普通软件BUG修复工作，仅执行致命问题修复、安全类问题修复以及升级等操作。
停止服务 (EOS)	指停止云服务版本的使用，现网版本需要升级到新的云服务版本。

MRS新版本发布后，EOM时间为版本发布后2年，EOFS在EOM后1年，EOS在EOFS后0.5年。

例如2024-03-30发布MRS 3.3.1-LTS版本，则该版本EOM时间为2026-03-30，EOFS为2027-03-30，EOS为2027-09-30。

表 2-2 MRS 普通版本生命周期表

版本名称	状态	发布时间	停止销售日	停止全面支持日	停止服务日
MRS 1.3.x	EOS	2017.3.30	2019.3.30	2020.3.30	2020.9.30
MRS 1.5.x	EOS	2017.9.30	2019.9.30	2020.9.30	2021.3.30
MRS 1.6.x	EOS	2019.6.21	2021.6.21	2022.6.21	2022.12.30
MRS 1.7.x	EOS	2019.12.22	2021.12.22	2022.12.22	2023.6.22
MRS 1.8.x	EOS	2019.11.21	2021.11.21	2022.11.21	2023.5.21
MRS 1.9.x	EOS	2020.3.8	2022.3.8	2023.3.8	2023.9.8
MRS 2.0.x	EOS	2019.10.11	2021.10.11	2022.10.11	2023.4.11
MRS 2.1.x	EOS	2019.11.13	2021.11.13	2022.11.13	2023.5.13
FusionInsight 6.5.1	EOS	2020.6.30	2022.6.30	2023.6.30	2023.12.30
MRS 3.0.x	EOS	2020.9.28	2022.9.28	2023.9.28	2024.3.28
MRS 3.1.0	EOFS	2021.5.9	2023.5.9	2024.5.9	2024.11.9
MRS 3.1.1	EOFS	2021.6.28	2023.6.28	2024.6.28	2024.12.28
MRS 3.1.2	EOM	2022.1.27	2024.1.27	2025.1.27	2025.7.27
MRS 3.1.5	已发布	2023.3.28	2025.3.28	2026.3.28	2026.9.28

📖 说明

以上表格中加粗的版本为现网全网开放的主力版本，其他版本为受限白名单方式开放，需联系技术支持申请白名单开通。

表 2-3 MRS LTS 版本生命周期表

版本名称	状态	发布时间	停止销售日	停止全面支持日	停止服务日
MRS 3.1.0-LTS	EOFS	2021.3.26	2023.3.26	2024.3.26	2024.9.26
MRS 3.1.1-LTS	EOFS	2021.6.28	2023.6.28	2024.6.28	2024.12.28
MRS 3.1.2-LTS	已发布	2022.6.2	2024.6.2	2025.6.2	2025.12.2

版本名称	状态	发布时间	停止销售日	停止全面支持日	停止服务日
MRS 3.1.3-LTS	已发布	2023.5.12	2025.5.12	2026.5.12	2026.11.12
MRS 3.2.0-LTS	已发布	2023.4.27	2025.4.27	2026.4.27	2026.10.27
MRS 3.3.0-LTS	已发布	2023.10.13	2025.10.13	2026.10.13	2027.4.13
MRS 3.3.1-LTS	已发布	2024.4.30	2026.4.30	2027.4.30	2027.10.30

📖 说明

以上表格中加粗的版本为现网全网开放的主力版本，其他版本为受限白名单方式开放，需联系技术支持申请白名单开通。

补充说明：

由于历史版本的EOS时间较早，已经EOS的版本将提供过渡期服务支持截止至2024年8月30日，即在2024年8月30日之后EOS的版本停止提供服务。

版本 EOX 后的建议策略

- 版本升级：MRS LTS版集群支持原地版本升级能力，可参考具体的版本升级路径进行按需升级。
- 集群迁移：MRS普通版集群不支持原地升级，建议用户将集群迁移至最新的在网版本。