



Red Hat Fuse 7.13

Red Hat Fuse 7.13 发行注记

Red Hat Fuse 的新内容

Red Hat Fuse 的新内容

法律通告

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

摘要

这些备注提供了 Red Hat Fuse 版本之间的变化概述。

目录

使开源包含更多	3
第 1 章 FUSE 7.13 产品概述	4
1.1. FUSE 分发	4
1.2. 支持的配置	4
第 2 章 OPENSIFT 上的 FUSE	5
2.1. 支持的 OPENSIFT 版本	5
2.2. 支持的镜像	5
第 3 章 FUSE STANDALONE	7
3.1. 支持的容器	7
3.2. 技术预览功能	7
3.3. FUSE 7.13 的 BOM 文件	9
第 4 章 弃用和删除的功能	10
4.1. 已弃用	10
4.2. 在 FUSE 7.11 中删除	10
4.3. 在 FUSE 7.10 中删除	11
4.4. 在 FUSE 7.8 中删除	11
4.5. 在 FUSE 7.5 中删除	11
4.6. 在 FUSE 7.3 中删除	11
4.7. 在 FUSE 7.2 中删除	12
4.8. 在 FUSE 7.0 中删除	12
4.9. 在 FUSE 7.0 中替换	13
第 5 章 FUSE 7.13 中不支持的功能	14
第 6 章 已知问题	15
6.1. CVE 安全漏洞	15
6.2. OPENSIFT 上的 FUSE	18
6.3. APACHE KARAF 上的 FUSE	19
6.4. JBOSS EAP 上的 FUSE	19
6.5. SPRING BOOT 上的 FUSE	20
6.6. FUSE 工具	20
6.7. APACHE CAMEL	21
第 7 章 修复了 FUSE 7.13 中的问题	22
7.1. 在 FUSE 7.13 中解决的错误	22

使开源包含更多

红帽致力于替换我们的代码、文档和 Web 属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。这些更改将在即将发行的几个发行本中逐渐实施。详情请查看我们的 [CTO Chris Wright 信息](#)。

第 1 章 FUSE 7.13 产品概述

1.1. FUSE 分发

Fuse 7.13 以两种不同的发行版的形式提供，如下所示：

Fuse 独立

在多个操作系统上支持的 Fuse 的经典分发。以下容器类型支持以下发行版本：

- Apache Karaf
- JBoss Enterprise Application Platform (EAP)
- Spring Boot

OpenShift 上的 Fuse

在 OpenShift 上运行集成应用程序的 Fuse 发行版（在 Red Hat Enterprise Linux 操作系统上支持）。在这种情况下，支持的容器类型以 docker 格式的容器镜像的形式提供：

- Java 镜像（用于 Spring Boot）
- Apache Karaf 镜像
- JBoss EAP 镜像

1.2. 支持的配置



重要

对于使用 Java 8 在 Karaf 上运行 Fuse 的用户，建议使用 OpenJDK 8u282 或 OpenJDK 8u302。不要使用 OpenJDK 8u292，它有一个影响凭证存储的已知问题（请参阅 [ENTESB-16417](#)）。OracleJDK 1.8.0_291 也会受到此问题的影响。

有关版本 7.13 中支持的配置、标准和组件的详情，请查看以下客户门户网站文章：

- [Red Hat Fuse 支持的配置](#)
- [Red Hat Fuse 支持的标准](#)
- [Red Hat Fuse 组件详情](#)

第 2 章 OPENSIFT 上的 FUSE

OpenShift 上的 Fuse 可让您在 OpenShift Container Platform 上部署 Fuse 应用程序。

2.1. 支持的 OPENSIFT 版本

有关 OpenShift 上 Fuse 支持的 OpenShift Container Platform 版本（或版本）的详情，请查看 [支持的配置页面](#)。

2.2. 支持的镜像

OpenShift 上的 Fuse 提供以下 Docker 格式的镜像：

Image	平台	支持的构架
fuse7/fuse-java-openshift-rhel8	Spring Boot	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-java-openshift-jdk11-rhel8	Spring Boot	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-java-openshift-jdk17-rhel8	Spring Boot	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-java-openshift-openj9-11-rhel8	Spring Boot	IBM Z 和 LinuxONE (s390x) IBM Power Systems (ppc64le)
fuse7/fuse-karaf-openshift-rhel8	Apache Karaf	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-karaf-openshift-jdk11-rhel8	Apache Karaf	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-karaf-openshift-jdk17-rhel8	Apache Karaf	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-eap-openshift-jdk11-rhel8	Red Hat JBoss Enterprise Application Platform	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-eap-openshift-jdk17-rhel8	Red Hat JBoss Enterprise Application Platform	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-console-rhel8	Fuse 控制台	AMD64 和 Intel 64 (x86_64) IBM Z 和 LinuxONE (s390x) IBM Power Systems (ppc64le)
fuse7/fuse-console—rhel8-operator	Fuse console operator	AMD64 和 Intel 64 (x86_64) IBM Z 和 LinuxONE (s390x) IBM Power Systems (ppc64le)

Image	平台	支持的构架
fuse7/fuse-apicurito-generator-rhel8	Apicurito REST 应用生成器	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-apicurito-rhel8	Apicurito REST API 编辑器	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-apicurito-rhel8-operator	API Designer Operator	AMD64 和 Intel 64 (x86_64)

第 3 章 FUSE STANDALONE

3.1. 支持的容器

以下运行时容器支持 Fuse 独立 7.13 :

- Spring Boot 2 (standalone)
- Apache Karaf
- Red Hat JBoss Enterprise Application Platform (JBoss EAP)

3.2. 技术预览功能

Fuse 独立的以下功能 *只是技术预览*，在 Fuse 7.13 中不支持：

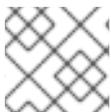
saga EIP

Saga Enterprise Integration Pattern (EIP)是一个技术预览功能，仅具有 *In-Memory Saga* 服务（不适用于生产环境）。不支持 LRA Saga 服务。如需了解更多详细信息，请参阅“[Apache Camel 开发指南](#)”中的 *Saga EIP* 部分。

3.2.1. Fuse Tooling 支持 Apache Camel

Fuse 工具为 Camel 应用程序开发提供了跨平台、跨 IDE 方法，支持 Visual Studio Code、Eclipse IDE 和 Eclipse Che 的 Apache Camel 语言支持扩展或插件。

Visual Studio Code 功能



注意

VS Code Apache Camel 扩展是社区功能。红帽不支持它们。

[Apache Camel 扩展的语言支持](#)为 Camel URI 提供功能，如下所示：

对于 XML DSL 和 Java DSL：

- 您可以在 VS Code outline 面板中导航到端点，并在 **Go > Go to Symbol in File** 导航面板中进入端点。
- 当您输入时，编辑器为 Camel 组件、属性和属性值列表提供代码完成。
- 将鼠标悬停在 Camel 组件上时，编辑器显示组件的简短描述（来自 [Apache Camel 组件参考](#)）。
- 编辑文件时，编辑器对 Camel 代码执行 Apache Camel 验证检查。
- 您可以选择 **File → Preferences → Settings → Apache Camel Tooling → Camel catalog version** 来指定特定的 Camel Catalog 版本。
- 您可以使用“Quick fix”功能来处理无效的 enum 值和未知 Camel URI 组件属性。

仅限 XML DSL：

- 您可以在 VS Code outline 面板中导航到 Camel 上下文和路由，并在 **File 导航面板中的 Go > Go to Symbol 中** 进入 Camel 上下文和路由。

- 当您输入时，编辑器为直接 ID、**直接虚拟机**、**虚拟机**和 **SEDA** 组件提供代码完成。
- 您可以在所有打开的 Camel 文件中找到 **直接** 和 **直接虚拟机** 组件的引用。

对于属性：

- Camel 组件属性的完成
- 诊断

要访问 **Apache Camel 功能的语言支持**，您可以添加一个或多个扩展。

[Apache Camel 扩展包安装](#) 以下 VS Code 扩展：

- [Apache Camel 的语言支持](#)
- [OpenShift Connector](#)
- [Java 扩展包](#)
- [Spring Boot 扩展软件包](#)
- [红帽项目初始化器](#)
- [XML 语言支持](#)
- [AtlasMap Data Transformation 编辑器](#)
- [Didact 教程](#)
- [Apache Camel K 工具](#)

另外，您可以单独安装扩展。

如需了解更多详细信息，请参阅以下 readme 文件：

- [Apache Camel 扩展包的 README](#)
- [Visual Studio Code 的 Apache Camel 语言服务器协议的 README](#)
- [README for AtlasMap Data Transformation 编辑器](#)

Eclipse IDE 功能

Apache Camel Eclipse 插件的语言支持为 Camel URI 提供以下功能：

在 XML DSL 和 Java DSL 的通用 Eclipse 文本编辑器中：

- 当您输入时，编辑器为 Camel 组件、属性和属性值列表提供代码完成。
- 将鼠标悬停在 Camel 组件上时，编辑器显示组件的简短描述（来自 [Apache Camel 组件参考](#)）。

要访问 **Apache Camel 功能的语言支持**，您可以从 Eclipse Marketplace 安装 Eclipse 插件。详情请查看 Eclipse IDE 的 Apache Camel 语言服务器协议的 [readme 文件](#)。

Eclipse Che 功能

Eclipse Che 7 的 **Apache Camel 插件的语言支持**在 XML DSL 和 Java DSL 中提供 Camel URI。

- 当您输入时，编辑器为 Camel 组件、属性和属性值列表提供代码完成。
- 将鼠标悬停在 Camel 组件上时，编辑器显示组件的简短描述（来自 [Apache Camel 组件参考](#)）。
- 保存文件时，编辑器对 Camel 代码执行 Apache Camel 验证检查。

要为 Eclipse Che 激活此插件，您可以使用 "Apache Camel based on Spring Boot" 堆栈或编辑工作区配置。

3.3. FUSE 7.13 的 BOM 文件

要将 Maven 项目配置为使用受支持的 Fuse 7.13 工件，请使用本节中记录的 BOM 版本。

3.3.1. BOM 文件用于 Fuse 7.13

要将 Fuse 独立应用程序升级到使用 7.13 依赖项，请编辑 Maven `pom.xml` 并更改下表中列出的 BOM 和 Maven 插件的版本：

表 3.1. 使用 BOM 的 7.13 的 Maven BOM 和插件版本

容器类型	Maven BOM 或 Plugin Artifact groupId/artifactId	Fuse 7.13 的版本
Spring Boot 2	org.jboss.redhat-fuse/fuse-springboot-bom	7.13.0.fuse-7_13_0-00012-redhat-00001
	org.jboss.redhat-fuse/spring-boot-maven-plugin	7.13.0.fuse-7_13_0-00012-redhat-00001
Apache Karaf	org.jboss.redhat-fuse/fuse-karaf-bom	7.13.0.fuse-7_13_0-00012-redhat-00001
	org.jboss.redhat-fuse/karaf-maven-plugin	7.13.0.fuse-7_13_0-00012-redhat-00001
JBoss EAP	org.jboss.redhat-fuse/fuse-eap-bom	7.13.0.fuse-7_13_0-00012-redhat-00001

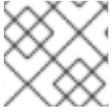
有关使用 BOM 的详情，请参阅 [迁移指南](#)。

第 4 章 弃用和删除的功能

如果您需要任何帮助，或者对 Fuse 7 中即将推出的更改有任何疑问，请联系 support@redhat.com。

4.1. 已弃用

Fuse 7.13 中弃用了以下功能，并可能在以后的版本中删除：



注意

Fuse Online 在 Fuse 7.13 中删除

对 iPXE 运行时和 JBoss Enterprise Application Platform (EAP) 的支持已弃用

当 Fuse 7 于 2024 年 6 月 30 日结束支持时，支持将停止支持，以及对 JBoss Enterprise Application Platform (EAP) 的支持。当 Fuse 7 结束支持时，Camel 将不再在 Karaf OSGi 或 JBoss EAP 上受到支持。

OpenWire 协议已弃用

从 Fuse 7.10 开始，使用 OpenWire 协议（可用于连接 AMQ Broker 实例）已弃用。请注意，自 AMQ Broker 版本 7.9.0 后，OpenWire 协议也被弃用。

wsdl2rest 工具已弃用

自 Fuse 7.10 起，**wsdl2rest** 命令行工具已被弃用。VS Code 的 WSDL 2 Camel Rest DSL 扩展也被弃用。

在 Camel 应用程序中弃用了 PHP、Python 和 Ruby 脚本语言

自 Fuse 7.4 起，PHP、Python 和 Ruby 脚本语言在 Camel 应用程序中被弃用，并将在以后的版本中删除。从 Camel 2.19 开始，Camel 社区已弃用 PHP、Python 和 Ruby（请参阅 [CAMEL-10973](#)）。这适用于所有 Fuse 容器类型：Apache Karaf、JBoss EAP 和 Spring Boot。

HP-UX OS 已被弃用

HP-UX 操作系统已被弃用，因为 Fuse 7.2 和对此操作系统的支持可能会在以后的 Fuse 发行版本中删除。特别是，JBoss EAP 7.2 容器已丢弃了对 HP-UX 的支持，因此任何在 JBoss EAP 7.2 上运行的 Fuse 版本都不支持在 HP-UX 上。

Camel MQTT 组件已弃用

Camel MQTT 组件在 Fuse 7.0 中已弃用，并将在以后的 Fuse 发行版本中删除。您可以使用 Camel Paho 组件，它使用流行的 [Eclipse Paho](#) 库来支持 MQTT 消息传递协议。

除了 Linux 外，Camel LevelDB 组件在所有操作系统中都已弃用

自 Fuse 6.3 起，Camel LevelDB (**camel-leveldb**) 组件在所有操作系统上已被弃用，但 Red Hat Enterprise Linux 除外。未来，Camel LevelDB 组件仅在 Red Hat Enterprise Linux 上被支持。

Camel SJMS 组件的 BatchMessage 类已弃用

Camel SJMS 组件的 BatchMessage 类在 Fuse 7 中被弃用（自 Apache Camel 2.17 起弃用），并可能从未来版本的 Apache Camel 和 Fuse 中删除。

4.2. 在 FUSE 7.11 中删除

在 OCP 3.11 上安装 Fuse Online

不支持在 OCP 3.11 上安装 Fuse 在线环境 7.13。在 OCP 3.11 上安装 Fuse Online 的 Fuse Online 已完全删除。

由 camel-ftp 和 camel-ssh 默认不支持 RSA/SHA-1 Ciphers

在 Fuse 7.11 中，**camel-ftp** 和 **camel-ssh** 组件将不再支持 RSA/SHA-1 密码的 TLS。依赖于 JSch 库的其他 Camel 组件也可能会受到影响。

如需更多信息，请参阅此 [红帽客户门户网站文章](#)。

4.3. 在 FUSE 7.10 中删除

fabric8-maven-plugin

fabric8-maven-plugin 已从 Fuse 7.10 中完全删除。我们建议您使用 **openshift-maven-plugin** 在 OpenShift 上的 Fuse 中构建和部署 Maven 项目。该插件由 Eclipse JKube 维护，它为插件提供了广泛的 [文档](#)。

4.4. 在 FUSE 7.8 中删除

Spring Boot 1

Fuse 7.8 不再支持 Spring Boot 1。建议您按照 [Spring Boot 2.0 迁移指南](#) 中的指导将 Spring Boot 应用程序迁移到 Spring Boot 2。

Fuse Online 中的 Camel K 运行时

Fuse 7.8 不再支持 Fuse Online 中的 Camel K 运行时（技术预览功能）。

Camel XmlJson 组件已在 7.8 中删除

Camel XmlJson (**camel-xmljson**) 组件已在 Fuse 7.8 中删除。

4.5. 在 FUSE 7.5 中删除

Fuse 7.5 中删除了以下功能：

7.5 中丢弃了对与 MS SQL Server 2014 集成的支持

MS SQL Server 2014 不再经过测试并支持与 Fuse 7.5 集成。我们建议您使用 MS SQL Server 最新版本，而不是 `awl-setuptools`，例如，MS SQL Server 2016 或 2017。

Camel LinkedIn 组件已在 7.5 中删除

在 Fuse 7.5 中删除了 **camel-linkedin** 组件。



重要

虽然从 Fuse 7.5 中删除，但 **camel-linkedin** 组件可能会在以后的发行版本中恢复。

4.6. 在 FUSE 7.3 中删除

Fuse 7.3 中删除了以下功能：

Camel YQL 组件已在 7.3 中删除

Camel YQL 组件已在 Fuse 7.3 中删除。

7.3 中已删除了 openjpa 和 OpenzFPC3 Karaf 功能

openjpa 功能和 **openjpa3** 功能已从 7.3 中的 Apache Karaf 容器中删除。对于 Java Persistence 架构 (diag) 实现，请使用支持的 **hibernate** 功能。

在 7.3 中删除了 **camel-jetty Karaf 功能**

camel-jetty 功能已从 7.3 中的 Apache Karaf 容器中删除，因为它使用 Jetty 8。改为使用 **camel-jetty9** 功能。

在 7.3 中删除了 Pax-jms-oracleaq Karaf 功能

pax-jms-oracleaq 功能已从 7.3 中的 Apache Karaf 容器中删除，因为它需要第三方非免费 Oracle AQ 库。

在 7.3 中，**camel-elasticsearch** 组件已从 EAP 上的 Fuse 中删除(Wildfly Camel)

camel-elasticsearch 组件已从 7.3 中的 EAP 上的 Fuse (Wildfly Camel) 中删除。改为使用较新的 **camel-elasticsearch-rest** 组件。

4.7. 在 FUSE 7.2 中删除

Fuse 7.2 中删除了以下功能：

Camel XMLRPC 组件已在 7.2 中删除

Camel XMLRPC 组件已在 Fuse 7.2 中删除。

Camel Netty 组件已在 7.2 中删除

Camel Netty 组件已在 Fuse 7.2 中删除。建议您改用 Camel Netty4 组件。

4.8. 在 FUSE 7.0 中删除

Fuse 7.0 中删除了以下功能：

7.0 中删除了对 Red Hat JBoss Operations Network (JON)的支持

自 Fuse 7.0 起，Flytron 上的 Fuse 不再支持 JON，不再提供用于与 JON 运行时集成的 JON 插件。

7.0 中删除了嵌入的 ActiveMQ 代理

自 Fuse 7.0 起，Fletl 上的 Fuse 不再提供嵌入式 ActiveMQ Broker。客户应直接连接到受支持的远程代理。有关我们支持的代理的更多信息，请参阅 [Red Hat Fuse 支持的配置](#) 页面中的 "支持消息传递提供程序" 部分。

7.0 中删除了 Fuse 集成包

对运行规则和流程的支持由 Red Hat JBoss BPM Suite 和 Red Hat JBoss BRMS 附带的组件提供。

7.0 中已删除用于子容器管理的 Karaf 控制台命令

自 Fuse 7.0 起，不支持用于子容器管理的 Karaf 控制台命令。也就是说，不支持以 **instance:** (Karaf 4.x 语法) 和前缀为 **admin:** (Karaf 2.x 语法) 的控制台命令。



注意

在 Fuse 7.0 GA 版本中，**instance:** 命令不会被删除。这是个已知问题。

7.0 中已删除了 SwitchYard

自 Fuse 7.0 起，drad 已被删除，您应该直接使用 Apache Camel。如需更多信息，请参阅 [Swoning Support Plan after Releasing Fuse 7](#)。

7.0 中删除了对 Fabric8 1.x 的支持

自 Fuse 7.0 起，Fabric8 v1 已被 OpenShift 上的 Fuse（以前为 Fuse 集成服务）替代，其中包括 Fabric8 v2 技术的组件。OpenShift 上的 Fuse 提供了一组工具和 Docker 格式镜像，支持 OpenShift 中集成微服务的开发、部署和管理。

虽然 OpenShift 上的 Fuse 具有不同的架构，但它满足 Fabric8 v1 提供的相同调配、自动化、中央配置和管理要求。如需更多信息，请参阅 [OpenShift 上的 Fuse 指南](#)。

7.0 中删除了 Google App Engine 的 Camel 组件

Fuse 7.0 中删除了 Google App Engine 的 Camel 组件(**camel-gae**)。

在 7.0 中删除了 Camel jBPM 组件

Camel jBPM 组件(**camel-jbpm**)已在 Fuse 7.0 中删除。

7.0 中删除了将 Fuse 安装为服务的 Tanuki 的打包程序

在 Fuse 7.0 中删除了基于 Tanuki 的 wrapper 脚本，使用 **wrapper:install** Karaf console command `iwl-wagon for` 将 Fuse 作为服务安装。要将 Apache Karaf 容器安装为一个服务，建议您改为使用 **bin/contrib** 目录中的新的 **karaf-service indices.sh** 脚本。

在 7.0 中删除了 Smooks

自 Fuse 7.0 起，Smooks 组件已删除。

在 7.0 中删除了 puppetlabs

VirtIO (基于 [Riftsaw](#) 项目) 已从 Fuse 7.0 中删除。如果您当前正在使用 `mvapich`，建议您考虑迁移到红帽 JBoss BPM 套件。

7.0 中删除了设计时间监管

Design Time Governance 组件已在 7.0 中删除。

7.0 中删除了运行时监管

自 Fuse 7.0 起，删除了 Runtime Governance (RTGov) 组件。

在 7.0 中删除 s-RAMP

Fuse 7.0 中删除了 SOA Repository Artifact Model and Protocol (S-RAMP) 组件。

bin/patch 脚本已在 7.0 中删除

在 Fuse 7.0 中删除了 **bin/patch** 脚本(**bin\patch.bat** on Windows O/S)。

7.0 不支持 Spring Dynamic Modules (Spring-DM)

Fuse 7.0 不支持 Spring XML 与 Apache Karaf 中的 OSGi 服务层集成，您应该改为使用 Blueprint 框架。使用 Blueprint XML 不会阻止您使用 Spring 框架中的 Java 库：最新版本的 Spring 与 Blueprint 兼容。

7.0 不支持 Apache Open JPA

Fuse 7.0 不支持 Java Persistence API (JPA) 的 [Apache Open JPA](#) 实现。建议您使用 [Hibernate](#) 实现。

4.9. 在 FUSE 7.0 中替换

Fuse 7.0 中替换了以下功能：

在 7.0 中已替换了 Geronimo 事务管理器

在 Fuse 7.0 中，Geronimo 容器中的 Geronimo 事务管理器已被 [Narayana](#) 替代。

jetty 容器已在 7.0 中被替换

在 Fuse 7.0 中，Jetty 容器已被 [Undertow](#) 替代。最初，此更改仅适用于 Jetty 容器的内部使用（例如，在 Karaf 容器中）。其他 Jetty 组件可能会在以后的版本中删除。

第 5 章 FUSE 7.13 中不支持的功能

Red Hat Fuse 7.13 不支持以下功能。

IBM PowerPC 和 Z 平台上的 Fuse 不支持 camel-leveldb 组件

当在 IBM PowerPC 或 IBM Z 平台上安装 Fuse 时，不支持 Camel LevelDB 组件。

OCP 3.11 不支持使用 Operator 安装 Fuse Console

不支持使用 Operator 安装 Fuse 控制台，且不适用于 OpenShift Container Platform (OCP) 3.11。在 OCP 3.11 上安装 Fuse Console 的建议方法是使用模板。

不支持 Apache Karaf EclipseLink 功能

Fuse 不支持 Apache Karaf EclipseLink 功能，因为此功能依赖于 JPA 2.2，而 Fuse 7.2 的 Karaf 容器与 JPA 2.1 一致。

不支持 Apache Aries Blueprint Web 模块

Fuse 不支持 Apache Aries [Blueprint Web](#) 模块。在 Apache Camel 的社区版中存在一个包含 Blueprint Web 的示例（作为单独的下载提供）并不意味着 Fuse 中支持此功能。

Apache Camel on Apache Karaf 不支持 PHP 脚本语言

Apache Karaf 容器上的 Camel 应用程序不支持 PHP 脚本语言，因为 PHP 没有适用于 PHP 的 OSGi 捆绑包。PHP 脚本语言在 JBoss EAP 容器和 Spring Boot 容器中的 Camel 应用程序中被弃用。

Apache Camel on Apache Karaf 不支持 Python 脚本语言

Apache Karaf 容器上的 Camel 应用程序不支持 Python 脚本语言，因为 Python 没有适用于 Python 的 OSGi 捆绑包。Python 脚本语言在 JBoss EAP 容器和 Spring Boot 容器中的 Camel 应用程序中被弃用。

第 6 章 已知问题

以下小节描述了版本 7.13 中的已知问题。

6.1. CVE 安全漏洞

作为中间件集成平台，Fuse 可能会与大量第三方组件集成。无法始终排除 Fuse 的一些第三方依赖项可能会存在安全漏洞。本节记录了与影响 Fuse 7.13 第三方依赖项的安全性相关的已知常见漏洞和暴露 (CVE)。

CVE-2020-13936 CVE-2020-13936 velocity: 当攻击者能够修改模板时执行任意代码

可以修改 Velocity 模板的攻击者可以执行任意 Java 代码，或运行任意系统命令，其特权与运行 Servlet 容器的帐户相同。这适用于允许不受信任的用户上传/修改 velocity 模板的应用程序，这些模板运行 Apache Velocity Engine 版本（最多 2.2）。

Fuse 7.9（及更高版本）的依赖项可确保只使用防止此漏洞的固定的 Velocity 版本(2.3)。如果您的应用程序代码对 Apache Velocity 组件有明确的依赖项，我们建议您升级这些依赖项以使用固定版本。

CVE-2018-10237 CVE-2018-10237 guava: Unbounded memory allocation in AtomicDoubleArray 和 CompoundOrdering 类允许远程攻击者拒绝服务 [fuse-7.0.0]

Google Guava 版本 11.0 到 24.1 会受到 AtomicDoubleArray 类中未绑定的内存分配（当使用 Java 序列化序列化）和 CompoundOrdering 类（当使用 research 序列化序列化）中无限的内存分配。攻击者可以利用使用 Guava 和反序列化不序列化数据的应用程序，从而导致拒绝 service iwl-osgi。如需更多信息，请参阅 [CVE-2018-10237](#)。

要避免此安全漏洞，我们建议您：

- 从未知源不会反序列化 AtomicDoubleArray 实例或 CompoundOrdering 实例。
- 避免使用 Guava 版本 24 及更早版本（虽然在某些情况下无法避免早期版本）。

为了便于避免较早版本的 Guava，Fuse 7.7（及更高版本）版本已经为所有容器配置了 Maven Bill of Materials (BOM) 文件，以默认选择 Guava 27。这意味着，如果您在 Maven 项目中将 Fuse BOM 整合到 Maven 项目中（通过将 BOM 的依赖添加到 POM 文件的 dependencyManagement 部分），然后在没有指定显式版本的情况下指定 Guava 工件的依赖关系，Genava 版本将默认为 BOM 中指定的版本，即 Fuse 7.7 BOM 的版本 27。

但是，至少有一个常见的用例涉及 Apache Karaf (OSGi) 容器，在这种情况下，无法避免使用 Guava：如果您的 OSGi 应用程序使用 Guava 和 Swagger，则您很难使用 Guava 20，因为这是 Swagger 所需的版本。在这里我们解释为什么如此，以及如何配置 POM 文件来恢复之前(vulnerable) Genava 20 库。首先，您需要了解双 OSGi 链的概念。

双 OSGi 链

OSGi 运行时中的捆绑包使用软件包约束（软件包名称+ 可选版本/范围）来连接 together，以及 exports。每个捆绑包可以有多个导入，通常那些导入一个带有多个捆绑包的捆绑包。例如：

```
BundleA
+-- BundleB
|  +-- BundleCa
+-- BundleCb
```

其中 BundleA 依赖于 BundleB 和 BundleCb，而 BundleB 则依赖于 BundleCa。BundleCa 和 BundleCb 应相同捆绑包，如果导出相同的软件包，但由于版本（范围）约束，BundleB 使用(有线)与 BundleA 不同的修订版本/版本 BundleC。

重写前面的图，以反映应用程序中的 Guava 和 Swagger 的依赖关系时发生的情况：

```
org.jboss.qe.cxf.rs.swagger-deployment
+-- Guava 27
+-- Swagger 1.5
    +-- reflections 0.9.11
        +-- Guava 20
```

如果您尝试部署此捆绑包配置，您会收到错误 `org.osgi.framework.BundleException: Uses constraint violation`。

恢复到 Guava 20

如果您的项目同时使用 Guava 和 Swagger 库（直接或间接），您应该将 `maven-bundle-plugin` 配置为对 Guava 捆绑包导入使用显式版本范围（或根本没有范围），如下所示：

```
<Import-Package>
  com.google.common.base;version="[20.0,21.0)",
  com.google.common.collect;version="[20.0,21.0)",
  com.google.common.io;version="[20.0,21.0)"
</Import-Package>
```

此配置会强制您的 OSGi 应用程序恢复到(vulnerable) Guava 20 库。因此，在这种情况下，务必要避免反序列化 `AtomicDoubleArray` 实例。

CVE-2017-12629 Solr/Lucene -security 绕过访问敏感数据 - CVE-2017-12629

Apache Solr 是一个流行的开源搜索平台，它使用 Apache Lucene 搜索引擎。如果您的应用程序使用 Apache Solr 与 Apache Lucene（例如，使用 Camel Solr 组件）的 Apache Solr 的组合，则可能会受此安全漏洞的影响。有关此漏洞的详情以及要采取的缓解方案，请参阅链接的安全公告。



注意

Fuse 运行时不直接使用 Apache Solr 或 Apache Lucene。只有在集成应用程序上下文中同时使用 Apache Solr 和 Apache Lucene 时（例如，使用 Camel Solr 组件时），才会出现安全风险。

CVE-2021-30129 mina-sshd-core: 在 Apache Mina SSHD 服务器中内存泄漏拒绝服务

Apache Mina SSHD 的 `sshd-core` 中的漏洞允许攻击者溢出服务器导致 `OutOfMemory` 错误。此问题会影响 Apache Mina SSHD 版本 2.0.0 及更新版本的 SFTP 和端口转发功能。它在 Apache Mina SSHD 2.7.0 中解决

Apache Mina SSHD 中的此漏洞由 [SSHD-1004](#) 解决，它弃用了存在此漏洞的某些加密算法。在 JBoss EAP 上的 Fuse 7.10 和 Fuse 7.10 中，这些已弃用的算法仍被支持（出于向后兼容性的原因）。但是，如果您使用这些已弃用的算法之一，强烈建议您重构应用程序代码以使用不同的算法。

在 Fuse 7.10 中，默认的加密算法已更改，如下所示：

Fuse 7.9	Fuse 7.10	在 Fuse 7.10 中被弃用？
aes128-ctr	aes128-ctr	
	aes192-ctr	

Fuse 7.9	Fuse 7.10	在 Fuse 7.10 中被弃用？
	aes256-ctr	
	aes128-gcm@openssh.com	
	aes256-gcm@openssh.com	
arcfour128	arcfour128	是
aes128-cbc	aes128-cbc	
	aes192-cbc	
	aes256-cbc	
3des-cbc	3des-cbc	是
Blowfish-cbc	Blowfish-cbc	是

在 Fuse 7.10 中，默认的密钥交换算法已更改，如下所示：

Fuse 7.9	Fuse 7.10	在 7.10 中被弃用？
diffie-hellman-group-exchange-sha256	diffie-hellman-group-exchange-sha256	
ecdh-sha2-nistp521	ecdh-sha2-nistp521	
ecdh-sha2-nistp384	ecdh-sha2-nistp384	
ecdh-sha2-nistp256	ecdh-sha2-nistp256	
	diffie-hellman-group18-sha512	
	diffie-hellman-group17-sha512	
	diffie-hellman-group16-sha512	
	diffie-hellman-group15-sha512	
	diffie-hellman-group14-sha256	

Fuse 7.9	Fuse 7.10	在 7.10 中被弃用？
diffie-hellman-group-exchange-sha1	diffie-hellman-group-exchange-sha1	是
diffie-hellman-group1-sha1	diffie-hellman-group1-sha1	是

6.2. OPENSIFT 上的 FUSE

本节列出了影响在 OpenShift 中部署 Fuse 应用程序的问题。有关影响特定容器的问题详情，请参阅 Spring Boot、Apache Karaf 上的 Fuse 部分，以及 JBoss EAP 上的 Fuse。OpenShift 发行版上的 Fuse 有以下已知问题：

ENTESB-21281 使用 add-opens 更新 FoO 镜像

在 Open Shift 上没有 add-opens Fuse 无法与 jdk17 正常工作。这些标志无法自动交付，因此您必须通过将标志添加到定义附加组件的脚本来自行指定。

自 Java 17 起，Java 平台模块系统是强制的。它实施强大的封装，以限制访问。您可以使用 --add-opens 选项允许访问，提供深度反映，并允许指定的模块打开 named 软件包：

```
--add-opens module/package=target-module(,target-module)*
```

ENTESB-21281 [Fuse on Openshift] QS karaf-cxf-rest - JavaDoc 不再支持 jdk17

Red Hat FUSE 7.x 中的 cxf java2wadl-plugin 不适用于 JDK17。

ENTESB-17895 [Fuse Console] 升级订阅不会更新 Hawtio

在 Fuse 7.10 中，如果您通过将 Operator 订阅频道更改为版本 7.10 来更新 Fuse 控制台，Fuse Console 会保留在 version 7.9 上。即使 Fuse Console 容器和 pod 具有标签 7.10，它们仍然使用 7.9 镜像。要临时解决这个问题，请通过删除旧版本的 Fuse 控制台来执行升级，然后进行全新的 Fuse Console 版本 7.10 安装。

ENTESB-17861 Apicurito generator 无法生成 Fuse Camel 项目

在 Fuse 7.10 中，如果 API Designer (Apicurito) 通过 Apicurito Operator 安装 (giving a Invalid Cert Error) 安装它无法正常工作。要临时解决这个问题：

1. 打开一个新标签页，进入 <https://apicurito-service-generator-apicurito.apps.cluster-name.openshift.com> (将 cluster-name.openshift.com 替换为集群名称。)
2. 接受证书。
3. 切换到应用程序，然后再次单击 generate 按钮。

ENTESB-17836 [Fuse Console] 在 Camel 树中不会显示新添加的路由

在 Fuse 7.10 中，部署应用程序后，Fuse Console 上的 Camel 树中不会显示路由（或路由）。您可以通过刷新页面来解决此问题，这应该会显示路由。

OCF 上的 ENTESB-19351 FIPS - Jolokia 代理因为不支持的安全编码而没有启动

在启用了 OCF FIPS 的 Jolokia 代理中的 Fuse 7.11 中，因为不支持的安全编码而不可用。

OCF 上的 [ENTESB-19352](#) FIPS - karaf-maven-plugin assembly 目标无法不支持的安全供应商

在 Fuse 7.11 中，如果我们使用带有 assembly 目标的 karaf-maven-plugin，则二进制流部署策略在启用了 OCF FIPS 时失败。

6.3. APACHE KARAF 上的 FUSE

Apache Karaf 上的 Fuse 有以下已知问题：

[ENTESB-16417](#) 凭证存储默认使用 PBEWithSHA1AndDESede

OpenJDK 8u292 和 OracleJDK 1.8.0_291 中的安全 API 返回不完整的安全提供程序列表，这会导致 Apache Karaf 中的凭证存储失败（因为所需的安全供应商似乎不可用）。导致此问题的根本问题是 <https://bugs.openjdk.java.net/browse/JDK-8249906>。我们建议您使用早期的 OpenJDK 版本、OpenJDK 8u282 或更新的 OpenJDK 版本 OpenJDK 8u302，它们没有这个程序错误。

Windows 上的 [ENTESB-16526](#) fuse-karaf 无法在补丁期间重启：install

在 Windows 平台上的 Apache Karaf 容器中运行 patch:install 时，在某些情况下，在 patch:install 命令尝试自动重启容器时可能会遇到以下错误：

```
Red Hat Fuse starting up. Press Enter to open the shell now...
100%
[=====]
Karaf started in 18s. Bundle stats: 235 active, 235 total
'.tmpdir' is not recognized as an internal or external command,
operable program or batch file.
There is a Root instance already running with name ~14 and pid ~13. If you know what you are
doing and want to force the run anyway, SET CHECK_ROOT_INSTANCE_RUNNING=false and
re run the command.
```

如果您遇到此错误，只需手动重新启动 Karaf 容器。

[ENTESB-8140](#) Start 级别热部署捆绑包默认为 80

从 Fuse 7.0 GA 版本开始，在 Apache Karaf 容器中，热部署的捆绑包的开始级别默认为 80。这可能会导致热部署捆绑包出现问题，因为有很多系统捆绑包和功能具有相同的启动级别。要临时解决这个问题，并确保热部署的捆绑包可靠地启动，请编辑 etc/org.apache.felix.fileinstall-deploy.cfg 文件并更改 felix.fileinstall.start.level 设置，如下所示：

```
felix.fileinstall.start.level = 90
```

[ENTESB-7664](#) 安装框架安全特性终止 karaf

必须使用 --no-auto-refresh 选项安装 framework-security OSGi 功能，否则此功能将关闭 Apache Karaf 容器。例如：

```
feature:install -v --no-auto-refresh framework-security
```

6.4. JBOSS EAP 上的 FUSE

JBoss EAP 上的 Fuse 有以下已知问题：

[ENTESB-21314](#) [EAP 上的 Fuse] 支持 jdk17 模块

在 EAP 上没有 add-opens Fuse 无法与 jdk17 正常工作。这些标志无法自动交付，因此您必须通过将标志添加到定义附加组件的脚本来自行指定。

自 Java 17 起, [Java 平台模块系统](#) 是强制的。它实施强大的封装, 以 [限制访问](#)。您可以使用 `--add-opens` 选项允许访问, 提供深度反映, 并允许指定的模块打开 named 软件包:

```
--add-opens module/package=target-module(,target-module)*
```

为 jdk17 删除了 [ENTESB-20833](#) `java.security.acl.Group`

`java.security.acl.Group` 在 jdk14 或更高版本中删除。

EAP 域模式上的 [ENTESB-13168](#) Camel 部署无法在 Windows 上工作

从 Fuse 7.6.0 开始, 对于 JBoss EAP 上的 Fuse, 在 Windows OS 上的域模式中无法部署 Camel 子系统。

6.5. SPRING BOOT 上的 FUSE

Spring Boot 上的 Fuse 有以下已知问题:

[ENTESB-21315](#) [在 Spring-boot 上使用支持 jdk17 模块

如果没有附加打开 Fuse, 则无法与 jdk17 正常工作。这些标志无法自动交付, 因此您必须通过将标志添加到定义附加组件的脚本来自行指定。

自 Java 17 起, [Java 平台模块系统](#) 是强制的。它实施强大的封装, 以 [限制访问](#)。您可以使用 `--add-opens` 选项允许访问, 提供深度反映, 并允许指定的模块打开 named 软件包:

```
--add-opens module/package=target-module(,target-module)*
```

[ENTESB-21421](#) / [ENTESB-20842](#) Spring Boot 2.6 不允许循环依赖项

Spring Boot 2.6 可能无法解析循环依赖项。如果您在 Spring Boot 中使用 XML DSL 来实例化 beans 文件中的自定义 `HealthCheckRegistry`, 则构建会失败。

作为临时解决方案, 您可以将属性 `spring.main.allow-circular-references=true` 添加到 `application.properties`。

6.6. FUSE 工具

Fuse 工具有以下已知问题:

[ENTESB-20965](#) [Hawtio] Login failed due: no LoginModules 为 hawtio-domain

Hawtio 只能使用 WildFly 的旧安全系统。如果您试图使用 Elytron 安全性登录到 Hawtio, 控制台会显示以下出错信息。

```
11:30:21,039 WARN [io.hawt.system.Authenticator] (default task-2) Login failed due to: No LoginModules configured for hawtio-domain
```

[ENTESB-19668](#) 当客户端证书身份验证被拒绝时, Hawtio 管理控制台不会在 UI 上显示消息

在拒绝来自客户端证书的身份验证后, Hawtio 组件不会在登录页面上显示任何消息。Hawtio 仅将网页浏览器重定向到登录页面, 而不显示任何消息。

[ENTESB-17705](#) [Hawtio] Logout 按钮会消失

在 Fuse 7.10 中, 登录并注销一行内多次后, 不会显示 Logout 按钮。要临时解决这个问题, 您可以刷新页面一次或多次, Logout 按钮应该重新应用。

[ENTESB-17839](#) Fuse + AtlasMap: Unrecognized field "dataSourceType"

在 Fuse 7.11 中，如果用户想要使用 AtlasMap vscode 扩展，那么他们必须使用 0.0.9 版本，因为 Fuse 7.11 与 AtlasMap 2.3.x 使用。否则，请使用 AtlasMap standalone 2.3.x，但不使用 vscode-extension。

6.7. APACHE CAMEL

Apache Camel 有以下已知问题：

ENTESB-19361/UNDERTOW-2206 Access logging support by cxf with embedded undertow server on karaf 不记录 URI

如果 `DECODE_URL` 选项为 `true`（这是 Fuse 7.11.1 karaf 运行时的默认值），并使用 `HttpServerExchange` 来解码 `relativePath` 和 `requestPath`，则 `requestURI` 参数保持编码。分配方法(转发，包括 `async` 和 `error`)分配路径而不解码，对于 `requestPath` 和 `relativeURL`，这会导致分配给路径，如 `/some%20thing`。

ENTESB-15343 XSLT 组件无法与 IBM1.8 JDK 正常工作

在 Fuse 7.8 中，Camel XSLT 组件无法与 IBM 1.8 JDK 正常工作。出现这个问题的原因是，XSLT 的 Apache Xerces 实现不支持 `javax.xml.XMLConstants#FEATURE_SECURE_PROCESSING` 属性（请参阅 [XERCESJ-1654](#)）。

ENTESB-11060 [camel-linkedin] V1 API 不再被支持

自 Fuse 7.4.0 起，Camel LinkedIn 组件无法再与 LinkedIn 服务器通信，因为它使用 LinkedIn Version 1.0 API 实施，它不再受 LinkedIn 支持。Camel LinkedIn 组件将更新为在以后的 Fuse 版本中使用 Version 2 API。

ENTESB-7469 Camel Docker 组件无法在 EAP 上使用 Unix 套接字连接

自 Fuse 7.0 起，`camel-docker` 组件只能通过其 REST API 连接到 Docker，而不通过 UNIX 套接字连接。

ENTESB-5231 PHP 脚本语言无法正常工作

Apache Karaf 容器上的 Camel 应用程序不支持 PHP 脚本语言，因为 PHP 没有适用于 PHP 的 OSGi 捆绑包。

ENTESB-5232 Python 语言无法正常工作

Apache Karaf 容器上的 Camel 应用程序不支持 Python 脚本语言，因为 Python 没有适用于 Python 的 OSGi 捆绑包。

ENTESB-2443 Google Mail API - 发送消息和草案不是同步

当您发送消息或草案时，响应包含一个 ID 的 Message 对象。可能无法通过另一个调用 API 立即获取此消息。您可能需要等待和重试调用。

ENTESB-2332 Google Drive API JSON 响应用于更改返回首页的项目的错误计数

Google Drive API JSON 响应用于更改返回首页的项目的错误计数。为列表操作设置 `maxResults` 可能无法返回第一个页面中的所有结果。您可能需要通过多个页面来获取完整的列表（即在新请求中设置 `pageToken`）。

第 7 章 修复了 FUSE 7.13 中的问题

以下小节列出了 Fuse 7.13 中修复的问题：

- [第 7.1 节“在 Fuse 7.13 中解决的错误”](#)

7.1. 在 FUSE 7.13 中解决的错误

下表列出了 Fuse 7.13 中已解析的错误。

表 7.1. Fuse 7.13 解决的错误

问题	描述
ENTESB-22629	Fuse 7.12 蓝图属性没有解决
ENTESB-22511	Infinispan-hibernate-cache-commons 在 fuse 7.12.1 bom 中未定义
ENTESB-22498	如果在 onException 块中设置了 "handled true", 则 <doCatch> 块中设置的事务回滚无法正常工作
ENTESB-22490	用于 camel 2.x 的后向端口 CAMEL-13092
ENTESB-22375	CAMEL-11750 没有在 Fuse 中完全实施
ENTESB-22272	Karaf 启动期间的例外： java.lang.IllegalStateException: Resource has no uri
ENTESB-22175	camel-openapi-java RestModelConverters.processSchema () 忽略 Swagger @Schema 注解
ENTESB-21958	camel-http4 HttpComponent 日志原始密码不安全字符
ENTESB-21878	当日志记录处于 WARN 级别时， NullPointerException
ENTESB-21874	对于 PollEnrich File 组件， CamelBatchComplete 始终为 true
ENTESB-21858	使用 JDK 11.0.20 时将不开始
ENTESB-21776	Openshift 镜像上的 Fuse 使用非常旧的 jmx_prometheus_javaagent.jar
ENTESB-21763	带有 toD 的 camel-http4 无法在 Karaf 上工作
ENTESB-21757	[JDG-4351][JBMAR-235] camel-infinispan 需要从 2.0.9.Final 到 2.0.11.Final 的 jboss-marshalling 更新。
ENTESB-21756	改进 JSch 库的日志记录
ENTESB-21752	获取错误"应用程序上下文中某些 Bean 的依赖项， 形成一个循环"

问题	描述
ENTESB-21742	新的 Fuse 控制台部署在一年后无法正常工作"openshift-service-serving-signer"证书轮转
ENTESB-20503	构建失败并显示 "-Dorg.slf4j.simpleLogger.defaultLogLevel=trace" 选项
ENTESB-22700	CVE-2024-22201 jetty: stop 接受有效客户端的新连接 [fuse-7]
ENTESB-22698	CVE-2024-22243 springframework: URL Parsing with Host Validation [fuse-7]
ENTESB-22514	CVE-2024-21733 tomcat : 在默认错误页面 [fuse-7] 中调整不相关的请求正文 [fuse-7]
ENTESB-22510	CVE-2023-46749 shiro : 路径遍历攻击可能会导致绕过 [fuse-7]
ENTESB-22509	CVE-2023-50290 solr: : Apache Solr: 主机变量通过 Metrics API [fuse-7] 发布。
ENTESB-22385	CVE-2023-6481 logback: logback receiver [fuse-7] 中的序列化漏洞
ENTESB-22384	CVE-2023-6378 logback: serialization vulnerability in logback receiver [fuse-7]
ENTESB-22381	CVE-2022-41678 activemq: Apache ActiveMQ: Deserialization vulnerability on Jolokia, 它允许经过身份验证的用户执行 RCE [fuse-7]
ENTESB-22379	CVE-2023-46589 tomcat: HTTP 请求通过格式格式的 trailer 标头 [fuse-7] smuggling
ENTESB-22376	CVE-2023-34055 spring-boot: org.springframework.boot:spring-boot-actuator 类易受拒绝服务 [fuse-7]
ENTESB-22373	CVE-2023-33202 bcpxix: bc-java: Out of memory while resolve ASN.1 crafted data in org.bouncycastle.openssl.PEMParser class [fuse-7]
ENTESB-22280	CVE-2023-5072 JSON-java: parser混淆会导致 OOM [fuse-7]
ENTESB-22715	CVE-2024-22257 spring-security: Broken Access Control with Direct Use of AuthenticatedVoter [fuse-7]
ENTESB-22712	CVE-2024-22259 springframework: URL Parsing with Host Validation [fuse-7]
ENTESB-22719	CVE-2024-28752 cxf-core: Apache CXF SSRF 漏洞使用 Aegis databinding [fuse-7]

问题	描述
ENTESB-22356	CVE-2023-36478 http2-hpack: jetty: hpack header 值会导致在 http/2 [fuse-7] 中拒绝服务
ENTESB-22164	CVE-2023-39410 avro: apache-avro: Apache Avro Java SDK: Memory when deserializing untrusted data in Avro Java SDK [fuse-7]
ENTESB-22877	CVE-2024-30171 org.bouncycastle-bcprov-jdk18on: BouncyCastle 易受 Bleichenbacher (Marvin Attack)[fuse-7] 的影响。
ENTESB-21854	CVE-2023-3223 undertow: OutOfMemoryError due due due to @MultipartConfig 处理 [fuse-7]
ENTESB-21956	CVE-2023-40167 jetty-http: jetty: Improper validation of HTTP/1 content-length [fuse-7]
ENTESB-21953	CVE-2023-36479 jetty-servlets: jetty: Improper added of quotation marks to user inputs in CgiServlet [fuse-7]