



Red Hat Fuse 7.12

Release Notes for Red Hat Fuse 7.12

What's new in Red Hat Fuse

Red Hat Fuse 7.12 Release Notes for Red Hat Fuse 7.12

What's new in Red Hat Fuse

Legal Notice

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.

Abstract

These notes provide an overview of the changes between Red Hat Fuse releases.

Table of Contents

| | |
|---|-----------|
| MAKING OPEN SOURCE MORE INCLUSIVE | 4 |
| CHAPTER 1. FUSE 7.12 PRODUCT OVERVIEW | 5 |
| 1.1. FUSE DISTRIBUTIONS | 5 |
| 1.2. IMPORTANT NOTES | 5 |
| 1.3. SUPPORTED CONFIGURATIONS | 6 |
| CHAPTER 2. FUSE ONLINE | 7 |
| 2.1. ABOUT FUSE ONLINE DISTRIBUTIONS | 7 |
| 2.2. UPGRADING FROM FUSE ONLINE 7.11.X TO 7.12.X REQUIRES MANUAL UPGRADE STEPS | 7 |
| 2.3. UPGRADING FUSE ONLINE INTEGRATIONS | 8 |
| 2.4. IMPORTANT NOTES FOR FUSE ONLINE | 8 |
| 2.4.1. Adding Fuse Online monitoring resources (Prometheus and Grafana) on OCP 4.9 (or later) | 9 |
| 2.5. OBTAINING TECHNICAL SUPPORT FOR FUSE ONLINE | 13 |
| 2.6. TECHNOLOGY PREVIEW FEATURES IN FUSE ONLINE | 13 |
| CHAPTER 3. FUSE ON OPENSIFT | 15 |
| 3.1. SUPPORTED VERSION OF OPENSIFT | 15 |
| 3.2. SUPPORTED IMAGES | 15 |
| 3.3. NEW FEATURES IN FUSE 7.12 ON OPENSIFT | 16 |
| 3.4. IMPORTANT NOTES | 16 |
| CHAPTER 4. FUSE STANDALONE | 18 |
| 4.1. SUPPORTED CONTAINERS | 18 |
| 4.2. NEW FEATURES IN FUSE 7.12 | 18 |
| 4.3. TECHNOLOGY PREVIEW FEATURES | 18 |
| 4.3.1. Fuse Tooling support for Apache Camel | 18 |
| 4.4. BOM FILES FOR FUSE 7.12 | 20 |
| 4.4.1. BOM File for Fuse 7.12 | 20 |
| 4.4.2. BOM files for Fuse 7.12.1 | 21 |
| 4.5. IMPORTANT NOTES | 21 |
| CHAPTER 5. DEPRECATED AND REMOVED FEATURES | 23 |
| 5.1. DEPRECATED | 23 |
| 5.2. REMOVED IN FUSE 7.11 | 24 |
| 5.3. REMOVED IN FUSE 7.10 | 24 |
| 5.4. REMOVED IN FUSE 7.8 | 24 |
| 5.5. REMOVED IN FUSE 7.5 | 24 |
| 5.6. REMOVED IN FUSE 7.3 | 25 |
| 5.7. REMOVED IN FUSE 7.2 | 25 |
| 5.8. REMOVED IN FUSE 7.0 | 25 |
| 5.9. REPLACED IN FUSE 7.0 | 27 |
| CHAPTER 6. UNSUPPORTED FEATURES IN FUSE 7.12 | 28 |
| CHAPTER 7. KNOWN ISSUES | 29 |
| 7.1. CVE SECURITY VULNERABILITIES | 29 |
| 7.2. FUSE ONLINE | 32 |
| 7.3. FUSE ON OPENSIFT | 33 |
| 7.4. FUSE ON APACHE KARAF | 34 |
| 7.5. FUSE ON JBOSS EAP | 34 |
| 7.6. FUSE ON SPRING BOOT | 35 |
| 7.7. FUSE TOOLING | 35 |

| | |
|---|-----------|
| 7.8. APACHE CAMEL | 36 |
| CHAPTER 8. FIXED ISSUES IN FUSE 7.12 | 38 |
| 8.1. ENHANCEMENTS IN FUSE 7.12 | 38 |
| 8.2. COMPONENT UPGRADES IN FUSE 7.12 | 38 |
| 8.3. BUGS RESOLVED IN FUSE 7.12 | 38 |
| 8.4. BUGS RESOLVED IN FUSE 7.12.1 | 45 |

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our [CTO Chris Wright's message](#).

CHAPTER 1. FUSE 7.12 PRODUCT OVERVIEW

1.1. FUSE DISTRIBUTIONS

Fuse 7.12 is provided in the form of three different distributions, as follows:

Fuse standalone

The classic distribution of Fuse, supported on multiple operating systems. This distribution is supported for the following container types:

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

Fuse on OpenShift

The distribution of Fuse for running integration applications on OpenShift (supported on the Red Hat Enterprise Linux operating system). In this case, the supported container types are provided in the form of docker-formatted container images:

- Java image (for Spring Boot)
- Apache Karaf image
- JBoss EAP image

Fuse Online

The distribution of Fuse for non-expert integrators with a simplified workflow accessed through a browser based UI. This distribution is available for the following kinds of deployment:

- On an OpenShift Dedicated (OSD) cluster.
- For installation on an on-premises OpenShift cluster

1.2. IMPORTANT NOTES

Upgrade from JUnit 4 to JUnit5

Red Hat Fuse 7.12 uses Spring Boot 2.7.x which upgrades the JUnit 4 to JUnit 5. All the projects that use Fuse Spring Boot BOM 7.12 are dependent on JUnit 5. Customers migrating from Fuse 7.x to Fuse 7.12 may find that the unit tests running on Fuse on Spring Boot are no longer executed as part of the Maven build. To resolve this, add the relevant dependency to **maven-surefire-plugin** configuration as shown below.

```
<plugin>
<groupId>org.apache.maven.plugins</groupId>
<artifactId>maven-surefire-plugin</artifactId>
<version>${maven-surefire-plugin.version}</version>
<configuration>
<testFailureIgnore>true</testFailureIgnore>
</configuration>
<dependencies>
```

```
<dependency>
  <groupId>org.apache.maven.surefire</groupId>
  <artifactId>surefire-junit47</artifactId>
  <version>${maven-surefire-plugin.version}</version>
</dependency>
</dependencies>
</plugin>
```

For more information about migrating from JUnit4 see [Migrating from JUnit 4](#).

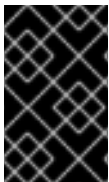
CVE-2020-8908 guava

A temp directory creation vulnerability exist in Guava versions prior to 30.0. We recommend updating Guava to version 30.0 or later, or update to Java 7 or later, or to explicitly change the permissions after the creation of the directory if neither are possible.

Red Hat CodeReady studio is scheduled for sunset

Red Hat CodeReady studio is scheduled for sunset. [JBoss Tools](#)(community) is the succeeding toolkit.

1.3. SUPPORTED CONFIGURATIONS



IMPORTANT

For running Fuse in Apache Karaf, we recommend OpenJDK 8u282 or OpenJDK 8u302. Do not use OpenJDK 8u292, which has a known issue affecting the credential store (see [ENTESB-16417](#)). OracleJDK 1.8.0_291 is also affected by this issue.

For information about supported configurations, standards, and components in version 7.12, see the following Customer Portal articles:

- [Red Hat Fuse Supported Configurations](#)
- [Red Hat Fuse Supported Standards](#)
- [Red Hat Fuse Component Details](#)

CHAPTER 2. FUSE ONLINE

Fuse Online provides a web browser interface that lets a business expert integrate two or more different applications or services without writing code. It also provides features that allow the addition of code if it is needed for complex use cases.

Fuse Online runs an integration on OpenShift as a Spring Boot application that uses Apache Camel.

2.1. ABOUT FUSE ONLINE DISTRIBUTIONS

Fuse Online is Red Hat's web-based integration platform. [Syndesis](#) is the open source project for Fuse Online. Fuse Online runs in these OpenShift environments:

| Host Environment | Installation |
|------------------------------|--|
| OpenShift Dedicated | Red Hat installs and provisions Fuse Online on Red Hat infrastructure. |
| OpenShift Container Platform | Customer installs and manages. |

2.2. UPGRADING FROM FUSE ONLINE 7.11.X TO 7.12.X REQUIRES MANUAL UPGRADE STEPS

If you installed Fuse Online 7.11.x and want to upgrade to Fuse Online 7.12.x.x, you must manually upgrade to Fuse Online 7.12.x.0.

1. In the **Administrator** perspective of the OpenShift Container Platform web console, navigate to **Operators > Installed Operators**.
2. Click the **Red Hat Integration Fuse Online 7.11.2** Operator.
3. Click the **Subscription** tab.
4. Verify that **Update approval** is set to **Manual**:
 - If **Update approval** is set to **Manual**, skip to the next step.
 - If **Update approval** is set to **Automatic**:
 - a. Click **Automatic**.
 - b. In the **Change Update Approval Strategy** dialog, select **Manual** and click **Save**.
5. Under **Update channel**, click **7.11.2**.
6. For the **Change subscription update channel**, select **7.12.x**.

Note: The **latest**, **candidate**, and **stable** channels are Technology Preview features.
7. Under **Upgrade status**, click **Upgrade available**.
8. Click **Preview InstallPlan** and then **Approve**.
9. Verify that the operator has fully completed the upgrade to Fuse Online 7.12.0:

- a. Navigate to the **Operators > Installed Operators** page and click **Red Hat Integration Fuse Online**. The **Operator Details** page opens.
 - b. Select the **Syndesis** tab. The status for the Fuse Online instance (the default name is **app**) initially shows **Installed** (to indicate that Fuse Online 7.12.0 is installed). It then progresses through several phases (**Installing**, **Starting**, and **Installed**). When it reaches the **Installed** phase again, the upgrade to 7.12.0 is complete.
10. Navigate back to the **Operators > Installed Operators** page, and then click **Upgrade available** for the **Red Hat Integration Fuse Online** operator.
11. Click **Preview InstallPlan** and then **Approve**.
12. Verify that the operator has fully completed the upgrade to Fuse Online 7.12.x:
 - a. Navigate to **Networking > Routes** and click on the location link for **syndesis** to open the Fuse Online web console.
 - b. In the upper right corner of the Fuse Online console, click the **?** icon and then select **About**.
 - c. Verify that the **About** page includes **7_12_x** in the version number.

2.3. UPGRADING FUSE ONLINE INTEGRATIONS

To upgrade a Fuse Online environment that is running on OCP on-site, you must update Fuse Online by using the operator and then republish any running integrations as described in [Upgrading Fuse Online](#).

On OCP 4.9 or later, when you upgrade to 7.11 by using the operator, the following warning is displayed during the Fuse Online Operator upgrade process:

W1219 18:38:58.064578 1 warnings.go:70] extensions/v1beta1 Ingress is deprecated in v1.14+, unavailable in v1.22+; use networking.k8s.io/v1 Ingress

This warning appears because clients (that Fuse Online uses for the Kubernetes/OpenShift API initialization code) access a deprecated Ingress version. This warning is *not* an indicator of complete use of deprecated APIs and there is no issue with upgrading to Fuse Online 7.11.

2.4. IMPORTANT NOTES FOR FUSE ONLINE

Important notes for the Fuse 7.12 release of the Fuse Online distribution:

- Support for Fuse Online is now deprecated as Fuse 7 is now in the maintenance support. There will not be any future development for Fuse Online when Fuse 7 moves out of support.
- Installation of Fuse Online is no longer supported on OCP 3.11.
- Fuse Online no longer supports Camel K runtime or the KNative connector.
- When Fuse Online is installed and provisioned on Red Hat infrastructure, the account is limited to a specific number of integrations that can be running at one time. For details, see the pricing plan.
- An OpenAPI schema that you upload to Fuse Online might not define input/output types. When Fuse Online creates a custom API client from an OpenAPI schema that does not specify input/output types then it is not possible to create an integration that maps integration data to fields that the API client can process or from fields that the API client processed. If an

integration requires data mapping to or from a custom API, then when you upload the OpenAPI schema, click **Review/Edit** to open API Designer, which is an API editing tool, and add input/output type specifications.

- Since Fuse 7.8, an OpenAPI document that you use for a custom API client connector or for an API provider integration cannot have cyclic schema references. For example, a JSON schema that specifies a request or response body cannot reference itself as a whole nor reference any part of itself through any number of intermediate schemas.
- On OCP 4.9 (or later), the **application-monitoring** project no longer works. It is a prerequisite for monitoring Fuse Online integrations and infrastructure components with Prometheus and Grafana.

To work around this issue, you can use the [built-in monitoring stack](#) (in the **openshift-monitoring** namespace) to use the **openshift-user-workload-monitoring** feature and the **grafana-operator** to use the **ops addon** as described in the following *Adding Fuse Online monitoring resources (Prometheus and Grafana) on OCP 4.9 (or later)* procedure.

2.4.1. Adding Fuse Online monitoring resources (Prometheus and Grafana) on OCP 4.9 (or later)

Prerequisites

- Fuse Online is installed and running on OCP 4.9 (or later) on-site.
- The **oc** client tool is installed and it is connected to the OCP cluster in which Fuse Online is installed.
- You have **admin** access to the OCP cluster.
- Your Fuse Online installation is configured with the **ops addon** enabled. If required, you can enable it with this command:

```
oc patch syndesis/app --type=merge -p '{"spec": {"addons": {"ops": {"enabled": true}}}]'
```

Procedure

1. If there is an existing **openshift-monitoring** configuration, skip to Step 2. Otherwise, create an **openshift-monitoring** configuration, that sets the user workload monitoring option to **true** and then skip to Step 3:

```
oc apply -f - <<EOF
apiVersion: v1
kind: ConfigMap
metadata:
  name: cluster-monitoring-config
  namespace: openshift-monitoring
data:
  config.yaml:
    enableUserWorkload: true
EOF
```

2. If there is an existing **openshift-monitoring** configuration:

- a. Check the existing **openshift-monitoring** configuration to determine whether the **user workload monitoring** option is set to **true**:

```
oc get -n openshift-monitoring cm/cluster-monitoring-config -
ojsonpath='{.data.config\.yaml}'
```

If the result is **enableUserWorkload: true**, the **user workload monitoring** option is set to **true**. Skip to Step 3.

If the result shows any other configurations, continue to the next step to enable the monitoring of user workloads by editing the ConfigMap.

- b. Open the ConfigMap file in an editor, for example:

```
oc -n openshift-monitoring edit cm/cluster-monitoring-config
```

- c. Set **enableUserWorkload** to **true**. For example:

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cluster-monitoring-config
  namespace: openshift-monitoring
data:
  config.yaml:
    enableUserWorkload: true
```

- d. Save the ConfigMap file.

3. Use the following command to watch the status of the pods in the **openshift-user-workload-monitoring** namespace:

```
oc -n openshift-user-workload-monitoring get pods -w
```

Wait until the status of the pods is Running, for example:

```
prometheus-operator-5d989f48fd-2qbzd 2/2 Running
prometheus-user-workload-0 5/5 Running prometheus-user-workload-1
5/5 Running
thanos-ruler-user-workload-0 3/3 Running
thanos-ruler-user-workload-1 3/3 Running
```

4. Verify that the Fuse Online alert rules are enabled in Prometheus:

- a. Access the internal prometheus instance

```
oc port-forward -n openshift-user-workload-monitoring pod/prometheus-user-workload-0
9090
```

- b. Open your browser to **localhost:9090**

- c. Select **Status> Targets**. You should see three **syndesis** endpoints.

- d. Press **CTRL-C** to terminate the **port-forward** process.

5. From the OperatorHub, install the Grafana Operator 4.1.0 to a namespace of your choosing, for example, to the **grafana-middleware** namespace.
6. Add a cluster role and a cluster role binding to allow the **grafana-operator** to list nodes and namespaces:
 - a. Download the cluster role YAML file from the **grafana-operator** website:

```
curl https://raw.githubusercontent.com/grafana-operator/grafana-operator/master/deploy/cluster_roles/cluster_role_grafana_operator.yaml > tmp_role.yaml
```

- b. Add cluster permission for the **grafana-operator** to read other namespaces and nodes:

```
cat <<EOF >> tmp_role.yaml
- apiGroups:
  - ""
  resources:
    - namespaces
    - nodes
  verbs:
    - get
    - list
    - watch
EOF
```

```
oc apply -f tmp_role.yaml
```

```
oc apply -f - <<EOF
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: grafana-operator
roleRef:
  name: grafana-operator
  kind: ClusterRole
  apiGroup: ""
subjects:
  - kind: ServiceAccount
    name: grafana-operator-controller-manager
    namespace: grafana-middleware
EOF
```

7. Enable the **grafana-operator** to read Grafana dashboards from other namespaces by using the **DASHBOARD_NAMESPACES_ALL** environment variable to limit the namespaces:

```
oc -n grafana-middleware patch subs/grafana-operator --type=merge -p '{"spec":{"config":{"env":[{"name":"DASHBOARD_NAMESPACES_ALL","value":"true"}]}}}'
```

8. Check that the **grafana** pods are recreated:

```
oc -n grafana-middleware get pods -w
```

9. Optionally, view the **grafana-operator** logs:

```
oc -n grafana-middleware logs -f `oc -n grafana-middleware get pods -oname|grep grafana-operator-controller-manager` -c manager
```

10. Add a [Grafana custom resource](#) to start a Grafana server pod, for example:

```
oc apply -f - <<EOF
apiVersion: integreatly.org/v1alpha1
kind: Grafana
metadata:
  name: grafana-middleware
  namespace: grafana-middleware
spec:
  config:
    auth:
      disable_signout_menu: true
    auth.anonymous:
      enabled: true
    log:
      level: warn
      mode: console
    security:
      admin_password: secret
      admin_user: root
    dashboardLabelSelector:
      - matchExpressions:
        - key: app
          operator: In
          values:
            - grafana
            - syndesis
    ingress:
      enabled: true
EOF
```

11. Allow the **grafana-operator** to read monitoring information:

```
oc -n grafana-middleware adm policy add-cluster-role-to-user cluster-monitoring-view -z grafana-serviceaccount
```

12. Add a **GrafanaDataSource** to query **thanos-querier**:

```
oc apply -f - <<EOF
apiVersion: integreatly.org/v1alpha1
kind: GrafanaDataSource
metadata:
  name: prometheus-grafanadatasource
  namespace: grafana-middleware
spec:
  datasources:
    - access: proxy
      editable: true
      isDefault: true
      jsonData:
        httpHeaderName1: 'Authorization'
      timeInterval: 5s
```



```

    tlsSkipVerify: true
    name: Prometheus
    secureJsonData:
      httpHeaderValue1: "Bearer $(oc -n grafana-middleware serviceaccounts get-token
grafana-serviceaccount)"
    type: prometheus
    url: "https://$(oc get route thanos-querier -n openshift-monitoring -
ojsonpath='{.spec.host}')"
    name: prometheus-grafanadatasource.yaml
EOF

```

13. View the grafana server log:

```
oc logs -f $(oc get pods -l app=grafana -o name)
```

14. Access the grafana URL and view the Fuse Online dashboards:

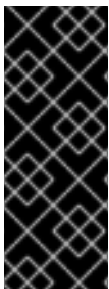
```
echo "https://$(oc -n grafana-middleware get route/grafana-route -ojsonpath='{.spec.host}')
```

2.5. OBTAINING TECHNICAL SUPPORT FOR FUSE ONLINE

To obtain technical support, in the Fuse Online console, in the left navigation panel, click **Support**. Use the **Support** page to download diagnostic information for all integrations or for one or more integrations that you choose. The page also provides a link for opening a support ticket and providing the diagnostic information that you downloaded.

2.6. TECHNOLOGY PREVIEW FEATURES IN FUSE ONLINE

This release includes the Technology Preview features that are listed below.



IMPORTANT

Technology Preview features are not supported with Red Hat production service level agreements (SLAs), might not be functionally complete, and Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process. For more information, see [Red Hat Technology Preview features support scope](#).

- **Fuse Online auditing**

Fuse Online supports basic auditing for changes made by any user to the following Fuse Online components:

- **Connections** – The **Name** and any other fields shown on the connector's **Details** page in the Fuse Online web console.
- **Connectors** – The **Name** field.
- **Integrations** – The **Name** field.

- [Conditional expressions for mapping data fields](#)

In the data mapper, you can specify a conditional expression and apply it to a data mapping. For example, a conditional expression can specify evaluation of a source field and how to populate

the target field if the source field is empty. The limited set of expressions that you can specify are similar to Microsoft Excel expressions.

- **Document scope for user-defined properties in data mapper**

In the data mapper, you can specify a scope for properties that you define for source and target mappings. In the **Mapping Details** panel, click **Add (+)** next to **Properties**. In the **Create Property** dialog, for the new **Scope** option, you can select the current message header, a message header from a previous step, or **Camel Exchange Property** for Camel-specific properties.

- **For a REST API client that uses OAuth** when you create an API client connector, you can change the default OAuth2 behavior of connections that you create from that connector. Fuse Online vendor extensions to the OpenAPI specification support the following:
 - Providing client credentials as parameters.
 - Obtaining a new access token based on HTTP response status codes.

CHAPTER 3. FUSE ON OPENSIFT

Fuse on OpenShift enables you to deploy Fuse applications on OpenShift Container Platform.

3.1. SUPPORTED VERSION OF OPENSIFT

For details of the supported version (or versions) of OpenShift Container Platform to use with Fuse on OpenShift, see the [Supported Configurations](#) page.

3.2. SUPPORTED IMAGES

Fuse on OpenShift provides the following Docker-formatted images:

| Image | Platform | Supported architectures |
|--|---|--|
| fuse7/fuse-java-openshift-rhel8 | Spring Boot | AMD64 and Intel 64 (x86_64) |
| fuse7/fuse-java-openshift-jdk11-rhel8 | Spring Boot | AMD64 and Intel 64 (x86_64) |
| fuse7/fuse-java-openshift-jdk17-rhel8 | Spring Boot | AMD64 and Intel 64 (x86_64) |
| fuse7/fuse-java-openshift-openj9-11-rhel8 | Spring Boot | IBM Z and LinuxONE (s390x) IBM Power Systems (ppc64le) |
| fuse7/fuse-karaf-openshift-rhel8 | Apache Karaf | AMD64 and Intel 64 (x86_64) |
| fuse7/fuse-karaf-openshift-jdk11-rhel8 | Apache Karaf | AMD64 and Intel 64 (x86_64) |
| fuse7/fuse-karaf-openshift-jdk17-rhel8 | Apache Karaf | AMD64 and Intel 64 (x86_64) |
| fuse7/fuse-eap-openshift-jdk8-rhel7 | Red Hat JBoss Enterprise Application Platform | AMD64 and Intel 64 (x86_64) |
| fuse7/fuse-eap-openshift-jdk11-rhel8 | Red Hat JBoss Enterprise Application Platform | AMD64 and Intel 64 (x86_64) |
| fuse7/fuse-eap-openshift-jdk17-rhel8 | Red Hat JBoss Enterprise Application Platform | AMD64 and Intel 64 (x86_64) |
| fuse7/fuse-console-rhel8 | Fuse console | AMD64 and Intel 64 (x86_64) IBM Z and LinuxONE (s390x) IBM Power Systems (ppc64le) |

| Image | Platform | Supported architectures |
|---|--------------------------------------|--|
| fuse7/fuse-console—rhel8-operator | Fuse console operator | AMD64 and Intel 64 (x86_64) IBM Z and LinuxONE (s390x) IBM Power Systems (ppc64le) |
| fuse7/fuse-apicurito-generator-rhel8 | Apicurito REST application generator | AMD64 and Intel 64 (x86_64) |
| fuse7/fuse-apicurito-rhel8 | Apicurito REST API editor | AMD64 and Intel 64 (x86_64) |
| fuse7/fuse-apicurito-rhel8-operator | API Designer Operator | AMD64 and Intel 64 (x86_64) |

3.3. NEW FEATURES IN FUSE 7.12 ON OPENSIFT

Fuse on OpenShift provides following new features in version 7.12:

- Support for JDK 17
Fuse 7.12 offers support for building the Fuse on OpenShift quickstarts using JDK 17.
- Running quickstarts with **openshift-maven-plugin**
Fuse 7.12 uses **openshift-maven-plugin** when building and running the Fuse on OpenShift quickstarts with Maven archtypes.
- Support for IBM Power Systems, IBM Z, and LinuxONE
Fuse 7.12 adds support for IBM Power Systems(ppc64le), IBM Z, and LinuxONE (s390x) on Red Hat OpenShift Container Platform 4.10 and later.



NOTE

In Fuse 7.12, installing the Fuse on OpenShift imagestreams and templates on IBM Power Systems, IBM Z, and LinuxONE is **not** supported. Only the components that can be installed with Fuse on OpenShift Operators are supported on IBM Power Systems, IBM Z, and LinuxONE.

3.4. IMPORTANT NOTES

Important notes for the Fuse 7.12 release of the Fuse on OpenShift distribution:

Support for Fuse 7.12 on OpenShift Container Platform (OCP) 4.11 or later

Fuse 7.12 contains updates that enable it to work with OpenShift Container Platform (OCP) 4.11 or later. If you plan to upgrade to OCP 4.11, you must upgrade Fuse to version 7.12 **before** you upgrade OCP to version 4.11. Earlier versions of Fuse (prior to 7.10) do not support OCP 4.9 or later.

Data Virtualization has been removed

Data Virtualization is deprecated since Fuse 7.7 and has been removed from Fuse 7.8.

Spring Boot 1 is has been removed

Spring Boot 1 is deprecated since Fuse 7.7 and has been removed from Fuse 7.8. We recommend that you migrate your Spring Boot applications to Spring Boot 2, following the guidance in the [Spring Boot 2.0 Migration Guide](#).

Fabric8 Maven plugin is removed

Fabric8 Maven plugin is completely removed from Fuse 7.10 and replaced with [OpenShift Maven plugin](#) since Fuse 7.10. Use OpenShift Maven plugin to build and deploy your applications.

Running quickstarts with JDK11

Use the correct JDK11 profile during the compile time if you want to use JDK11 based image at runtime. When building and deploying the quickstarts using JDK11, ensure that you have installed JDK11 on your build machine and then build your quickstarts using the correct JDK11 profile.

Changes in spring-boot artifact Id

In Fuse 7.12, Spring Boot is upgraded to 2.7.12.

Quickstart Spring-Boot RHOSAK fails because of spring-boot upgrade

The eap-camel-jpa quickstart has been removed

The **eap-camel-jpa** quickstart has been removed from Fuse 7.8 due to an issue with a dependency.

Jolokia not externally accessible since Fuse 7.8

Starting in Fuse 7.8, Jolokia default protocol is switched from HTTP to HTTPS.

FIPS-enabled Jolokia agent becomes unavailable

In OCP FIPS-enabled Jolokia agent becomes unavailable due to unsupported security encoding.

CHAPTER 4. FUSE STANDALONE

4.1. SUPPORTED CONTAINERS

Fuse standalone 7.12 is supported on the following runtime containers:

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

4.2. NEW FEATURES IN FUSE 7.12

The main new features of Fuse standalone in version 7.12 are:

Java 17 is supported

The Fuse 7.12 release supports Java 17, Java 11, and Java 8.

4.3. TECHNOLOGY PREVIEW FEATURES

The following features of Fuse standalone are *Technology Preview* only and are not supported in Fuse 7.12:

Saga EIP

The Saga Enterprise Integration Pattern (EIP) is a technology preview feature and features only the *In-Memory* Saga service (which is not suitable for a production environments). The LRA Saga service is *not* supported. For more details, see section [Saga EIP](#) of the "Apache Camel Development Guide".

4.3.1. Fuse Tooling support for Apache Camel

Fuse Tooling provides a cross-platform, cross-IDE approach to Camel application development, with Apache Camel language support extensions or plugins for Visual Studio Code, Eclipse IDE, and Eclipse Che.

Visual Studio Code features



NOTE

VS Code Apache Camel extensions are community features. They are not supported by Red Hat.

The [Language Support for Apache Camel](#) extension provides features for Camel URLs, such as the following:

For XML DSL and Java DSL:

- You can navigate to endpoints in the VS Code **Outline** panel and in the **Go > Go to Symbol in File** navigation panel.
- When you type, the editor provides code completion for Camel components, attributes, and the list of attribute values.

- When you hover over a Camel component, the editor shows a brief description of the component (from the [Apache Camel component reference](#)).
- As you edit the file, the editor performs an Apache Camel validation check on the Camel code.
- You can specify a specific Camel Catalog version by selecting **File → Preferences → Settings → Apache Camel Tooling → Camel catalog version**.
- You can use "Quick fix" features to address invalid enum values and unknown Camel URI component properties.

For XML DSL only:

- You can navigate to Camel contexts and routes in the VS Code **Outline** panel and in the **Go > Go to Symbol in File** navigation panel.
- When you type, the editor provides code completion for referenced IDs of **direct**, **direct VM**, **VM** and **SEDA** components.
- You can find references for **direct** and **direct VM** components in all open Camel files.

For Properties:

- Completion for Camel component property
- Diagnostic

To access the **Language Support for Apache Camel** features, you add one or more extensions.

The [Apache Camel Extension Pack](#) installs the following VS Code extensions:

- [Language Support for Apache Camel](#)
- [OpenShift Connector](#)
- [Java Extension Pack](#)
- [Spring Boot extension pack](#)
- [Project initializer by Red Hat](#)
- [XML Language Support](#)
- [AtlasMap Data Transformation editor](#)
- [Didact Tutorial](#)
- [Tooling for Apache Camel K](#)

Optionally, you can install the extensions individually.

For more details, see the following readme files:

- Readme for [Apache Camel Extension Pack](#)
- Readme for [Apache Camel Language Server Protocol for Visual Studio Code](#)
- Readme for [AtlasMap Data Transformation editor](#)

Eclipse IDE features

The **Language Support for Apache Camel** Eclipse plug-in provides the following features for Camel URIs:

In the generic Eclipse text editor for both XML DSL and Java DSL:

- When you type, the editor provides code completion for Camel components, attributes, and the list of attribute values.
- When you hover over a Camel component, the editor shows a brief description of the component (from the [Apache Camel component reference](#)).

To access the **Language Support for Apache Camel** features, you install the Eclipse plug-in from the Eclipse Marketplace. For more details, see the [readme file](#) for Apache Camel Language Server Protocol for Eclipse IDE.

Eclipse Che features

The **Language Support for Apache Camel** plugin for Eclipse Che 7 provides features for Camel URIs in XML DSL and Java DSL.

- When you type, the editor provides code completion for Camel components, attributes, and the list of attribute values.
- When you hover over a Camel component, the editor shows a brief description of the component (from the [Apache Camel component reference](#)).
- When you save the file, the editor performs an Apache Camel validation check on the Camel code.

To activate this plugin for Eclipse Che, you can use the "Apache Camel based on Spring Boot" stack or edit your workspace configuration.

4.4. BOM FILES FOR FUSE 7.12

To configure your Maven projects to use the supported Fuse 7.12 artifacts, use the BOM versions documented in this section.

4.4.1. BOM File for Fuse 7.12

To upgrade your Fuse standalone applications to use the 7.12 dependencies, edit the Maven **pom.xml** and change the versions of the BOMs and Maven plugins listed in the following table:

Table 4.1. Maven BOM and plugin versions for 7.12 using the BOM

| Container Type | Maven BOM or Plugin Artifact groupId/artifactId | Version for Fuse 7.12 |
|----------------|---|--|
| Spring Boot 2 | org.jboss.redhat-fuse/fuse-springboot-bom | 7.12.0.fuse-7_12_0-00016-redhat-00001 |
| | org.jboss.redhat-fuse/spring-boot-maven-plugin | 7.12.0.fuse-7_12_0-00016-redhat-00001 |

| Container Type | Maven BOM or Plugin Artifact groupId/artifactId | Version for Fuse 7.12 |
|----------------|---|--|
| Apache Karaf | org.jboss.redhat-fuse/fuse-karaf-bom | 7.12.0.fuse-7_12_0-00016-redhat-00001 |
| | org.jboss.redhat-fuse/karaf-maven-plugin | 7.12.0.fuse-7_12_0-00016-redhat-00001 |
| JBoss EAP | org.jboss.redhat-fuse/fuse-eap-bom | 7.12.0.fuse-7_12_0-00016-redhat-00001 |

For more details about using the BOM, see the [Migration Guide](#).

4.4.2. BOM files for Fuse 7.12.1

To configure your Maven projects to use the supported Fuse 7.12.1 artifacts, use the BOM versions documented in this section.

Table 4.2. Maven BOM and plugin versions for 7.12.1 using the BOM

| Container Type | Maven BOM or Plugin Artifact groupId/artifactId | Version for Fuse 7.12.1 |
|----------------|---|--|
| Spring Boot 2 | org.jboss.redhat-fuse/fuse-springboot-bom | 7.12.1.fuse-7_12_1-00009-redhat-00001 |
| | org.jboss.redhat-fuse/spring-boot-maven-plugin | 7.12.1.fuse-7_12_1-00009-redhat-00001 |
| Apache Karaf | org.jboss.redhat-fuse/fuse-karaf-bom | 7.12.1.fuse-7_12_1-00009-redhat-00001 |
| | org.jboss.redhat-fuse/karaf-maven-plugin | 7.12.1.fuse-7_12_1-00009-redhat-00001 |
| JBoss EAP | org.jboss.redhat-fuse/fuse-eap-bom | 7.12.1.fuse-7_12_1-00009-redhat-00001 |

For more details about using the BOM, see the [Migration Guide](#).

4.5. IMPORTANT NOTES

Important notes for the Fuse 7.12 release of the Fuse standalone distribution:

Java 17 is supported

The Fuse 7.12 release supports Java 17, Java 11, and Java 8.

Support for Karaf runtimes and JBoss EAP is deprecated

Support for Karaf runtimes and JBoss EAP is deprecated as Fuse 7 will move out of support with the release of Fuse 7.12.

Creating a connection to MongoDB using the MongoClientFactory

From Fuse 7.10 and later versions, use **com.mongodb.client.MongoClient** instead of **com.mongodb.MongoClient** to create a connection to MongoDB (note the extra *.client* sub-package in the full path).

This affects any user applications that use **camel-mongodb**, which will now need to create a connection bean as a **com.mongodb.client.MongoClient** instance. Moreover, the methods exposed by this class are not exactly the same as the old class which could require more refactoring of user code.

For example, create a connection to MongoDB as follows:

```
import com.mongodb.client.MongoClient;
```

You can then create the MongoClient bean as shown in following example:

```
return MongoClientFactory.create("mongodb://admin:password@192.168.99.102:32553");
```

CHAPTER 5. DEPRECATED AND REMOVED FEATURES

If you need any assistance or have any questions about the upcoming changes in Fuse 7, contact support@redhat.com.

5.1. DEPRECATED

The following features are deprecated in Fuse 7.12 and may be removed in a future release:

Support for Fuse Online is deprecated

Support for Fuse Online is now deprecated as Fuse 7 is now in the maintenance support. There will not be any future development for Fuse Online when Fuse 7 moves out of support.

Support for Karaf OSGi runtime and JBoss Enterprise Application Platform (EAP) is deprecated

support for the Karaf OSGi runtime and for JBoss Enterprise Application Platform (EAP) will stop when Fuse 7 moves out of support on June 30, 2024. Camel will no longer be supported on Karaf OSGi or JBoss EAP when Fuse 7 moves out of support.

OpenWire protocol is deprecated

Since Fuse 7.10, use of the OpenWire protocol (which could be used to connect AMQ Broker instances) is deprecated. Note that the OpenWire protocol is also deprecated in AMQ Broker since AMQ Broker version 7.9.0.

wsdl2rest tool is deprecated

Since Fuse 7.10, the **wsdl2rest** command line tool is deprecated. The WSDL 2 Camel Rest DSL extension for VS Code is also deprecated.

Fuse Online install script for installation on OCP 4

Since Fuse 7.8, the Fuse Online install script is deprecated for installing Fuse Online on OpenShift Container Platform (OCP) 4.x versions. On OCP 4.x versions, we recommend that you use the Fuse Online Operator.

PHP, Python, and Ruby scripting languages are deprecated in Camel applications

The PHP, Python, and Ruby scripting languages are deprecated in Camel applications since Fuse 7.4 and will be removed in a future release. The Camel community has deprecated PHP, Python, and Ruby since Camel 2.19 (see [CAMEL-10973](#)). This applies to all Fuse containers types: Apache Karaf, JBoss EAP, and Spring Boot.

HP-UX OS is deprecated

The HP-UX operating system is deprecated since Fuse 7.2 and support for this operating system could be removed in a future release of Fuse. In particular, note that the JBoss EAP 7.2 container has already dropped support for HP-UX and, consequently, any future version of Fuse on JBoss EAP that runs on JBoss EAP 7.2 will *not* be supported on HP-UX.

Camel MQTT component is deprecated

The Camel MQTT component is deprecated in Fuse 7.0 and will be removed in a future release of Fuse. You can use the Camel Paho component instead, which supports the MQTT messaging protocol using the popular [Eclipse Paho](#) library.

Camel LevelDB component is deprecated on all operating systems except for Linux

Since Fuse 6.3, the Camel LevelDB (**camel-leveldb**) component is deprecated on all operating systems except for Red Hat Enterprise Linux. In the future, the Camel LevelDB component will be supported only on Red Hat Enterprise Linux.

BatchMessage class from the Camel SJMS component is deprecated

The BatchMessage class from the Camel SJMS component is deprecated in Fuse 7 (deprecated in Apache Camel since version 2.17) and may be removed from a future version of Apache Camel and Fuse.

5.2. REMOVED IN FUSE 7.11

Installation of Fuse Online on OCP 3.11

Installing Fuse online environment 7.12 on OCP 3.11 is not supported. The Fuse Online install script is completely removed for installing Fuse Online on OCP 3.11.

RSA/SHA-1 Ciphers Not Supported by Default by camel-ftp and camel-ssh

From Fuse 7.11, the **camel-ftp** and **camel-ssh** components will no longer support TLS with RSA/SHA-1 cipher by default. Other Camel components that depend on the JSch library may also be affected.

For more information, see this [Red Hat Customer Portal Article](#) .

5.3. REMOVED IN FUSE 7.10

fabric8-maven-plugin

The **fabric8-maven-plugin** has been completely removed from Fuse 7.10. We recommend that you use the **openshift-maven-plugin** instead for building and deploying Maven projects in Fuse on OpenShift. The plugin is maintained by Eclipse JKube, which provides extensive [documentation](#) for the plugin.

5.4. REMOVED IN FUSE 7.8

Spring Boot 1

Spring Boot 1 is no longer supported in Fuse 7.8. We recommend that you migrate your Spring Boot applications to Spring Boot 2, following the guidance in the [Spring Boot 2.0 Migration Guide](#) .

Camel K runtime in Fuse Online

Camel K runtime in Fuse Online (technology preview feature) is no longer supported in Fuse 7.8.

Camel XmlJson component has been removed in 7.8

The Camel XmlJson (**camel-xmljson**) component has been removed in Fuse 7.8.

5.5. REMOVED IN FUSE 7.5

The following features were removed in Fuse 7.5:

Support for integration with MS SQL Server 2014 has been dropped in 7.5

MS SQL Server 2014 is no longer tested and supported for integrations with Fuse 7.5. We recommend that you use one of the more recent versions of MS SQL Server instead – for example, MS SQL Server 2016 or 2017.

Camel LinkedIn component has been removed in 7.5

The **camel-linkedin** component has been removed in Fuse 7.5.



IMPORTANT

Although removed from Fuse 7.5, the **camel-linkedin** component is likely to be restored in a later release.

5.6. REMOVED IN FUSE 7.3

The following features were removed in Fuse 7.3:

Camel YQL component has been removed in 7.3

The Camel YQL component has been removed in Fuse 7.3.

OpenJPA and OpenJPA3 Karaf features have been removed in 7.3

The **openjpa** feature and the **openjpa3** feature have been removed from the Apache Karaf container in 7.3. For a Java Persistence Architecture (JPA) implementation, use the supported **hibernate** feature instead.

camel-jetty Karaf feature has been removed in 7.3

The **camel-jetty** feature has been removed from the Apache Karaf container in 7.3, because it uses Jetty 8. Use the **camel-jetty9** feature instead.

pax-jms-oracleaq Karaf feature has been removed in 7.3

The **pax-jms-oracleaq** feature has been removed from the Apache Karaf container in 7.3, because it requires 3rd party, non-free Oracle AQ libraries.

camel-elasticsearch component has been removed from Fuse on EAP (Wildfly Camel) in 7.3

The **camel-elasticsearch** component has been removed from Fuse on EAP (Wildfly Camel) in 7.3. Use the newer **camel-elasticsearch-rest** component instead.

5.7. REMOVED IN FUSE 7.2

The following features were removed in Fuse 7.2:

Camel XMLRPC component has been removed in 7.2

The Camel XMLRPC component has been removed in Fuse 7.2.

Camel Netty component has been removed in 7.2

The Camel Netty component has been removed in Fuse 7.2. It is recommended that you use the Camel Netty4 component instead.

5.8. REMOVED IN FUSE 7.0

The following features were removed in Fuse 7.0:

Support for Red Hat JBoss Operations Network (JON) has been removed in 7.0

Since Fuse 7.0, Fuse on Karaf no longer supports JON and no longer provides JON plugins for integrating with the JON runtime.

Embedded ActiveMQ broker has been removed in 7.0

Since Fuse 7.0, Fuse on Karaf no longer provides an embedded ActiveMQ Broker. Customers should connect to a supported remote broker directly. For more information on our supported brokers, refer to the "Supported Messaging Providers" section of the [Red Hat Fuse Supported Configurations page](#).

Fuse integration pack has been removed in 7.0

Support for running rules and processes is provided by components shipped with Red Hat JBoss BPM Suite and Red Hat JBoss BRMS.

Karaf console commands for child container administration have been removed in 7.0

Since Fuse 7.0, the Karaf console commands for child container administration are *not* supported. That is, the console commands prefixed by **instance:** (Karaf 4.x syntax) and the console commands prefixed by **admin:** (Karaf 2.x syntax) are not supported.



NOTE

In the Fuse 7.0 GA release, the **instance:** commands are not removed. This is a known issue.

SwitchYard has been removed in 7.0

Since Fuse 7.0, SwitchYard has been removed, and you should use Apache Camel directly instead. For more detailed information, see the knowledge base article, [SwitchYard Support Plan After Releasing Fuse 7](#).

Support for Fabric8 1.x has been removed in 7.0

Since Fuse 7.0, Fabric8 v1 has been replaced by Fuse on OpenShift (previously, Fuse Integration Services), which includes components of Fabric8 v2 technology. Fuse on OpenShift provides a set of tools and Docker-formatted images that enable development, deployment, and management of integration microservices within OpenShift.

Although Fuse on OpenShift has a different architecture, it fulfills the same provisioning, automation, central configuration and management requirements that Fabric8 v1 provides. For more information, see [Fuse on OpenShift Guide](#).

Camel components for Google App Engine have been removed in 7.0

The Camel components for Google App Engine (**camel-gae**) have been removed in Fuse 7.0.

Camel jBPM component has been removed in 7.0

The Camel jBPM component (**camel-jbpm**) has been removed in Fuse 7.0.

Tanuki based wrapper for installing Fuse as a service has been removed in 7.0

The Tanuki based wrapper scripts – generated using the **wrapper:install** Karaf console command – for installing Fuse as a service have been removed in Fuse 7.0. To install the Apache Karaf container as a service, it is recommended that you use the new **karaf-service-*.sh** scripts from the **bin/contrib** directory instead.

Smooks has been removed in 7.0

Since Fuse 7.0, the Smooks component for SwitchYard has been removed.

BPEL has been removed in 7.0

BPEL (based on the [Riftsaw](#) project) has been removed from Fuse 7.0. If you are currently using BPEL, it is recommended that you consider migrating to the Red Hat JBoss BPM Suite.

Design Time Governance has been removed in 7.0

The Design Time Governance component has been removed in 7.0.

Runtime Governance has been removed in 7.0

Since Fuse 7.0, the Runtime Governance (RTGov) component has been removed.

S-RAMP has been removed in 7.0

The SOA Repository Artifact Model and Protocol (S-RAMP) component has been removed in Fuse 7.0.

bin/patch script has been removed in 7.0

The **bin/patch** script (**bin\patch.bat** on Windows O/S) has been removed in a Fuse 7.0.

Spring Dynamic Modules (Spring-DM) is not supported in 7.0

Spring-DM (which integrates Spring XML with the OSGi service layer in Apache Karaf) is not

supported in Fuse 7.0 and you should use the Blueprint framework instead. Using Blueprint XML does not prevent you from using the Java libraries from the Spring framework: the latest version of Spring is compatible with Blueprint.

Apache OpenJPA is not supported in 7.0

The [Apache OpenJPA](#) implementation of the Java Persistence API (JPA) is not supported in Fuse 7.0. It is recommended that you use the [Hibernate](#) implementation instead.

5.9. REPLACED IN FUSE 7.0

The following features were replaced in Fuse 7.0:

Geronimo transaction manager has been replaced in 7.0

In Fuse 7.0, the Geronimo transaction manager in the Karaf container has been replaced by [Narayana](#).

Jetty container has been replaced in 7.0

In Fuse 7.0, the Jetty container has been replaced by [Undertow](#). Initially, this change applies only to internal use of the Jetty container (for example, in the Karaf container). Other Jetty components might be removed in a future release.

CHAPTER 6. UNSUPPORTED FEATURES IN FUSE 7.12

The following features are unsupported in Red Hat Fuse 7.12.

camel-leveldb component is not supported for Fuse on the IBM PowerPC and Z platforms

When Fuse is installed on the IBM PowerPC or IBM Z platforms, the Camel LevelDB component is not supported.

Installing and running Fuse Online is not supported on OpenShift Container Platform (OCP) 3.11

Installing and running Fuse Online is not supported on OpenShift Container Platform (OCP) 3.11, since Fabric8 Maven Plugin is deprecated in favor of OpenShift Maven Plugin.

Installing Fuse Console using the Operator is not supported on OCP 3.11

Installing Fuse Console using the Operator is not supported and does not work on OpenShift Container Platform (OCP) 3.11. The recommended way to install Fuse Console on OCP 3.11 is to use templates.

Apache Karaf EclipseLink feature is unsupported

The Apache Karaf EclipseLink feature is **not** supported in Fuse, because this feature depends on JPA 2.2, while the Karaf container for Fuse 7.2 is aligned with JPA 2.1.

Apache Aries Blueprint Web module is unsupported

The Apache Aries [Blueprint Web](#) module is **not** supported in Fuse. The presence of an example featuring Blueprint Web in the community edition of Apache Camel (provided as a separate download) does **not** imply that this feature is supported in Fuse.

The PHP scripting language is not supported in Apache Camel on Apache Karaf

The PHP scripting language is **not** supported in Camel applications on the Apache Karaf container, because there is no OSGi bundle available for PHP. The PHP scripting language is deprecated in Camel applications on the JBoss EAP container and on the Spring Boot container.

The Python scripting language is not supported in Apache Camel on Apache Karaf

The Python scripting language is **not** supported in Camel applications on the Apache Karaf container, because there is no OSGi bundle available for Python. The Python scripting language is deprecated in Camel applications on the JBoss EAP container and on the Spring Boot container.

CHAPTER 7. KNOWN ISSUES

The following subsections describe the known issues in version 7.12.

7.1. CVE SECURITY VULNERABILITIES

As a middleware integration platform, Fuse can potentially be integrated with a large number of third-party components. It is not always possible to exclude the possibility that some third-party dependencies of Fuse could have security vulnerabilities. This section documents known common vulnerabilities and exposures (CVEs) related to security that affect third-party dependencies of Fuse 7.12.

[CVE-2020-13936](#) CVE-2020-13936 velocity: arbitrary code execution when attacker is able to modify templates

An attacker that is able to modify Velocity templates may execute arbitrary Java code or run arbitrary system commands with the same privileges as the account running the Servlet container. This applies to applications that allow untrusted users to upload/modify velocity templates running Apache Velocity Engine versions up to 2.2.

Dependencies for Fuse 7.9 (and later) ensure that it uses only the fixed Velocity version (2.3) that protects against this security vulnerability. If your application code has any explicit dependencies on the Apache Velocity component, we recommend that you upgrade these dependencies to use the fixed version.

[CVE-2018-10237](#) CVE-2018-10237 guava: Unbounded memory allocation in AtomicDoubleArray and CompoundOrdering classes allow remote attackers to cause a denial of service [fuse-7.0.0]

Google Guava versions 11.0 through 24.1 are vulnerable to unbounded memory allocation in the **AtomicDoubleArray** class (when serialized with Java serialization) and the **CompoundOrdering** class (when serialized with GWT serialization). An attacker could exploit applications that use Guava and deserialize untrusted data to cause a denial of service – for more details, see [CVE-2018-10237](#). To avoid this security vulnerability, we recommend that you:

- Never deserialize an **AtomicDoubleArray** instance or a **CompoundOrdering** instance from an unknown source.
- Avoid using Guava versions 24 and earlier (although in some cases it is not possible to avoid the earlier versions).

To make it easier to avoid the earlier (vulnerable) versions of Guava, Fuse 7.7 (and later) has configured its Maven Bill of Materials (BOM) files for all containers to select Guava 27 by default. This means that if you incorporate a Fuse BOM into your Maven project (by adding a dependency on the BOM to the **dependencyManagement** section of your POM file) and then specify a dependency on the Guava artifact *without* specifying an explicit version, the Guava version will default to the version specified in the BOM, which is version 27 for the Fuse 7.7 BOMs.

But there is at least one common use case involving the Apache Karaf (OSGi) container, where it is not possible to avoid using a vulnerable version of Guava: if your OSGi application uses Guava and Swagger together, you are obliged to use Guava 20, because that is the version required by Swagger. Here we explain why this is the case and how to configure your POM file to revert the earlier (vulnerable) Guava 20 library. First, you need to understand the concept of a *double OSGi chain*.

Double OSGi chain

Bundles in the OSGi runtime are *wired* together using package constraints (package name + optional version/range) – imports and exports. Each bundle can have multiple imports and usually those imports wire a given bundle with multiple bundles. For example:

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

Where **BundleA** depends on **BundleB** and **BundleCb**, while **BundleB** depends on **BundleCa**. **BundleCa** and **BundleCb** should be the same bundle, if they export the same packages, but due to version (range) constraints, **BundleB** uses (*wires to*) a different revision/version of **BundleC** than **BundleA**.

Rewriting the preceding diagram to reflect what happens when you include dependencies on both Guava and Swagger in an application:

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

If you try to deploy this bundle configuration, you get the error, **org.osgi.framework.BundleException: Uses constraint violation**.

Reverting to Guava 20

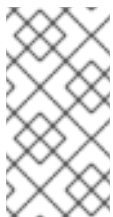
If your project uses both Guava and Swagger libraries (directly or indirectly), you should configure the **maven-bundle-plugin** to use an explicit version range (or no range at all) for the Guava bundle import, as follows:

```
<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>
```

This configuration forces your OSGi application to revert to the (vulnerable) Guava 20 library. It is therefore particularly important to avoid deserializing **AtomicDoubleArray** instances in this case.

[CVE-2017-12629](#) Solr/Lucene -security bypass to access sensitive data - CVE-2017-12629

Apache Solr is a popular open source search platform that uses the Apache Lucene search engine. If your application uses a combination of Apache Solr with Apache Lucene (for example, when using the Camel Solr component), it could be affected by this security vulnerability. Please consult the linked security advisory for more details of this vulnerability and the mitigation steps to take.



NOTE

The Fuse runtime does *not* use Apache Solr or Apache Lucene directly. The security risk only arises, if you are using Apache Solr and Apache Lucene together in the context of an integration application (for example, when using the Camel Solr component).

[CVE-2021-30129](#) mina-sshd-core: Memory leak denial of service in Apache Mina SSHD Server

A vulnerability in sshd-core of Apache Mina SSHD allows an attacker to overflow the server causing an OutOfMemory error. This issue affects the SFTP and port forwarding features of Apache Mina SSHD version 2.0.0 and later versions. It was addressed in Apache Mina SSHD 2.7.0

This vulnerability in Apache Mina SSHD was addressed by [SSHD-1004](#), which deprecates certain cryptographic algorithms that have this vulnerability. In Fuse 7.10 on Karaf and Fuse 7.10 on JBoss EAP, these deprecated algorithms are still supported (for reasons of backwards compatibility). However, if you are using one of these deprecated algorithms, it is strongly recommended that you refactor your application code to use a different algorithm instead.

In Fuse 7.10, the default cipher algorithms have changed as follows.

| Fuse 7.9 | Fuse 7.10 | Deprecated in Fuse 7.10? |
|---------------------|-------------------------------|--------------------------|
| aes128-ctr | aes128-ctr | |
| | aes192-ctr | |
| | aes256-ctr | |
| | aes128-gcm@openssh.com | |
| | aes256-gcm@openssh.com | |
| arcfour128 | arcfour128 | yes |
| aes128-cbc | aes128-cbc | |
| | aes192-cbc | |
| | aes256-cbc | |
| 3des-cbc | 3des-cbc | yes |
| blowfish-cbc | blowfish-cbc | yes |

In Fuse 7.10, the default key exchange algorithms have changed as follows.

| Fuse 7.9 | Fuse 7.10 | deprecated in 7.10? |
|---|---|---------------------|
| 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 | |

| Fuse 7.9 | Fuse 7.10 | deprecated in 7.10? |
|---|---|---------------------|
| | diffie-hellman-group18-sha512 | |
| | diffie-hellman-group17-sha512 | |
| | diffie-hellman-group16-sha512 | |
| | diffie-hellman-group15-sha512 | |
| | diffie-hellman-group14-sha256 | |
| diffie-hellman-group-exchange-sha1 | diffie-hellman-group-exchange-sha1 | yes |
| diffie-hellman-group1-sha1 | diffie-hellman-group1-sha1 | yes |

7.2. FUSE ONLINE

The Fuse Online distribution has the following known issues:

[ENTESB-21338](#) Twitter API v1.1 restrictions for new application

Any new Twitter application will not work due to Twitter v1.1 API restrictions.

[ENTESB-17674](#) Monitoring Fuse Online with Prometheus and Grafana on OCP 4.9 (or later) requires workaround

On OCP 4.9 (or later), the **application-monitoring** project no longer works. It is a prerequisite for monitoring Fuse Online integrations and infrastructure components with Prometheus and Grafana. To work around this issue, you can use the [built-in monitoring stack](#) (in the **openshift-monitoring** namespace) to use the **openshift-user-workload-monitoring** feature and the **grafana-operator** to use the **ops addon** as described in the **Important notes for Fuse Online** section of these release notes.

[ENTESB-14518](#) Jaeger operator installed by Syndesis 1.11 affects other namespaces

Since Fuse 7.8, when you install Fuse 7.8 Online (Syndesis 1.11) on an OpenShift cluster, the Jaeger Operator (which gets installed along with Fuse Online) is configured to manage *All namespaces* by default. A side effect of this behavior is that, in the case where you already have Fuse 7.7 Online (Syndesis 1.10) installed on a cluster and then you install Fuse 7.8 Online in a different namespace, the Jaeger Operator installed with Fuse 7.8 Online tries to manage the (older) Jaeger instance installed on the Fuse 7.7 Online namespace. The result is that a new **syndesis-jaeger** pod – in addition to the existing **syndesis-jaeger** pod – appears in the Fuse 7.7 Online namespace and the new **syndesis-jaeger** pod enters the **CrashLoopBackOff** state. The original Fuse 7.7 Online instance is not affected and the crashed **syndesis-jaeger** pod can be safely ignored.

[ENTESB-13966](#) Discovery of deployed integration API seems disabled but not really

Starting in Fuse 7.7, after creating a new integration containing an API, the integration detail page wrongly implies that 3scale discovery is disabled for this integration. Additionally, the integration detail page does not show the API URL. By clicking this button three times (click **Enable**, then click **Disable**, then click **Enable**), you can resynchronize the page so that 3scale discovery is enabled and the API URL is displayed.

7.3. FUSE ON OPENSIFT

This section lists issues that affect the deployment of Fuse applications on OpenShift. For details of issues affecting specific containers, see also the sections for Spring Boot, Fuse on Apache Karaf, and Fuse on JBoss EAP. The Fuse on OpenShift distribution has the following known issues:

ENTESB-21281 Update FoO images with add-opens

Without **add-opens** Fuse on Open Shift does not work properly with jdk17. These flags cannot be delivered automatically, so you have to specify them yourself, by adding the flags to a script that defines **add-opens**.

Since Java 17, the [Java Platform Module System](#) is *mandatory*. It implements strong encapsulation, which [restricts access](#). You can use the **--add-opens** option to allow access, providing deep reflection, and allowing a specified module to open the named package.:

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

ENTESB-21281 [Fuse on Openshift] QS karaf-cxf-rest - JavaDoc no longer supported on jdk17

The **cxf java2wadi-plugin** in Red Hat FUSE 7.x doesn't work with JDK17.

ENTESB-17895 [Fuse Console] Upgrade subscription does not update Hawtio

In Fuse 7.10, if you update the Fuse Console by changing the Operator subscription channel to version 7.10, the Fuse Console remains on version 7.9. Even if the Fuse Console containers and pods have the label 7.10, they are still using the 7.9 images. To work around this problem, perform the upgrade by removing the older version of Fuse Console and then making a fresh installation of Fuse Console version 7.10.

ENTESB-17861 Apicurito generator cannot generate Fuse Camel Project

In Fuse 7.10, the API Designer (Apicurito) does not work properly, if it is installed via the Apicurito Operator (giving an Invalid Cert Error). To work around this problem:

1. Open a new tab to **<https://apicurito-service-generator-apicurito.apps.cluster-name.openshift.com>**
(Replace **cluster-name.openshift.com** with your cluster name.)
2. Accept the certificates.
3. Switch to the application and click on the generate button again.

ENTESB-17836 [Fuse Console] A newly added route is not displayed in the Camel tree

In Fuse 7.10, after deploying an application, the route (or routes) is not displayed in the Camel tree on the Fuse Console. You can work around this issue by refreshing the page, which should make the route appear.

ENTESB-19351 FIPS on OCP - Jolokia agent doesn't start due to unsupported security encoding

In Fuse 7.11, in OCP FIPS-enabled Jolokia agent becomes unavailable due to unsupported security encoding.

[ENTESB-19352](#) FIPS on OCP - karaf-maven-plugin assembly goal fails to unsupported security provider

In Fuse 7.11, a binary stream deploy strategy fails on OCP FIPS enabled, with Karaf applications, if we use **karaf-maven-plugin** with assembly goal.

7.4. FUSE ON APACHE KARAF

Fuse on Apache Karaf has the following known issues:

[ENTESB-16417](#) Credential store is using PBESWithSHA1AndDESede by default

The security API in OpenJDK 8u292 and in OracleJDK 1.8.0_291 returns an incomplete list of security providers, which causes the credential store in Apache Karaf to fail (because the required security provider appears to be unavailable). The underlying issue that causes this problem is <https://bugs.openjdk.java.net/browse/JDK-8249906>. We recommend that you use the earlier OpenJDK version, OpenJDK 8u282, or the later OpenJDK version, OpenJDK 8u302, which do not have this bug.

[ENTESB-16526](#) fuse-karaf on Windows cannot restart during patch:install

While running **patch:install** in the Apache Karaf container on the Windows platform, under certain circumstances you might encounter the following error when the **patch:install** command attempts an automatic restart of the container:

```
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.
```

If you encounter this error, simply restart the Karaf container manually.

[ENTESB-8140](#) Start level of hot deploy bundles is 80 by default

Starting in the Fuse 7.0 GA release, in the Apache Karaf container the start level of hot deployed bundles is 80 by default. This can cause problems for the hot deployed bundles, because there are many system bundles and features that have the same start level. To work around this problem and ensure that hot deployed bundles start reliably, edit the **etc/org.apache.felix.fileinstall-deploy.cfg** file and change the **felix.fileinstall.start.level** setting as follows:

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

[ENTESB-7664](#) Installing framework-security feature kills karaf

The **framework-security** OSGi feature must be installed using the **--no-auto-refresh** option, otherwise this feature will shut down the Apache Karaf container. For example:

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

7.5. FUSE ON JBOSS EAP

Fuse on JBoss EAP has the following known issues:

ENTESB-21314 [Fuse on EAP] Support jdk17 modularity

Without **add-opens** Fuse on EAP does not work properly with jdk17. These flags cannot be delivered automatically, so you have to specify them yourself, by adding the flags to a script that defines **add-opens**.

Since Java 17, the [Java Platform Module System](#) is *mandatory*. It implements strong encapsulation, which [restricts access](#). You can use the **--add-opens** option to allow access, providing deep reflection, and allowing a specified module to open the named package.:

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

ENTESB-20833 java.security.acl.Group was removed for jdk17

java.security.acl.Group is removed in versions jdk14 or later.

ENTESB-13168 Camel deployment on EAP domain mode is not working on Windows

Starting in Fuse 7.6.0, for Fuse on JBoss EAP, the Camel subsystem cannot be deployed on JBoss EAP in domain mode on Windows OS.

7.6. FUSE ON SPRING BOOT

Fuse on Spring Boot has the following known issues:

ENTESB-21315 [Fuse on Spring-boot] Support jdk17 modularity

Without **add-opens** Fuse does not work properly with jdk17. These flags cannot be delivered automatically, so you have to specify them yourself, by adding the flags to a script that defines **add-opens**.

Since Java 17, the [Java Platform Module System](#) is *mandatory*. It implements strong encapsulation, which [restricts access](#). You can use the **--add-opens** option to allow access, providing deep reflection, and allowing a specified module to open the named package.:

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

ENTESB-21421/ENTESB-20842 Spring Boot 2.6 does not allow circular dependencies

Spring Boot 2.6 may be unable to resolve circular dependencies. If you use XML DSL in Spring Boot to instantiate a customized **HealthCheckRegistry** in your beans file, the build fails.

As a workaround, you can add the property **spring.main.allow-circular-references=true** to **application.properties**.

7.7. FUSE TOOLING

Fuse Tooling has the following known issues:

ENTESB-20965 [Hawtio] Login failed due to: No LoginModules configured for hawtio-domain

Hawtio can only work with the old security system with WildFly. If you attempt to login to Hawtio with Elytron security, the console displays the following error message.

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


ENTESB-19668 The Hawtio management console does not display a message on the UI when client certificate authentication is rejected

The Hawtio component does not show any message on the login page, after rejecting authentication from a client certificate. Hawtio only redirects the web browser to the login page, without showing any message.

ENTESB-17705 [Hawtio] Logout button disappears

In Fuse 7.10, after logging in and logging out several times in a row, the **Logout** button is not shown. To work around this issue, you can refresh the page one or more times and the **Logout** button should reappear.

ENTESB-17839 Fuse + AtlasMap: Unrecognized field "dataSourceType"

In Fuse 7.11, if user wants to use AtlasMap vscode extension, then they must use version 0.0.9 as Fuse 7.11 is with AtlasMap 2.3.x. Otherwise use AtlasMap standalone 2.3.x but not the vscode-extension.

7.8. APACHE CAMEL

Apache Camel has the following known issues:

ENTESB-19361 / UNDERTOW-2206 Access logging support by cxf with embedded undertow server on karaf does not log URI

If the **DECODE_URL** option is **true** (this is the default value for Fuse 7.11.1 karaf runtime), and use **HttpServerExchange** to decode **relativePath** and **requestPath**, the **requestURI** parameter remains encoded.

The dispatch methods (**forward**, **include**, **async** and **error**) assign the path without decoding it, for **requestPath** and **relativeURL**, which causes dispatching to a path such as **/some%20thing**.

ENTESB-15343 XSLT component not working properly with IBM1.8 JDK

In Fuse 7.8, the Camel XSLT component does not work properly with the IBM 1.8 JDK. The problem occurs because the underlying Apache Xerces implementation of XSLT does not support the **javax.xml.XMLConstants#FEATURE_SECURE_PROCESSING** property (see [XERCESJ-1654](#)).

ENTESB-11060 [camel-linkedin] V1 API is no longer supported

Since Fuse 7.4.0, the Camel LinkedIn component is no longer able to communicate with the LinkedIn server, because it is implemented using the LinkedIn Version 1.0 API, which is no longer supported by LinkedIn. The Camel LinkedIn component will be updated to use the Version 2 API in a future release of Fuse.

ENTESB-7469 Camel Docker component cannot use Unix socket connections on EAP

Since Fuse 7.0, the **camel-docker** component can connect to Docker only through its REST API, not through UNIX sockets.

ENTESB-5231 PHP script language does not work

The PHP scripting language is **not** supported in Camel applications on the Apache Karaf container, because there is no OSGi bundle available for PHP.

ENTESB-5232 Python language does not work

The Python scripting language is **not** supported in Camel applications on the Apache Karaf container, because there is no OSGi bundle available for Python.

ENTESB-2443 Google Mail API - Sending of messages and drafts is not synchronous

When you send a message or draft, the response contains a Message object with an ID. It may not be possible to immediately get this message via another call to the API. You may have to wait and retry the call.

ENTESB-2332 Google Drive API JSON response for changes returns bad count of items for the first page

Google Drive API JSON response for changes returns bad count of items for the first page. Setting **maxResults** for a list operation may not return all the results in the first page. You may have to go through several pages to get the complete list (that is by setting **pageToken** on new requests).

CHAPTER 8. FIXED ISSUES IN FUSE 7.12

The following sections list the issues that have been fixed in Fuse 7.12 and Fuse 7.12.1:

- [Section 8.1, “Enhancements in Fuse 7.12”](#)
- [Section 8.2, “Component Upgrades in Fuse 7.12”](#)
- [Section 8.3, “Bugs resolved in Fuse 7.12”](#)
- [Section 8.4, “Bugs resolved in Fuse 7.12.1”](#)

8.1. ENHANCEMENTS IN FUSE 7.12

| Issue | Description |
|------------------------------|--|
| ENTESB-17374 | Expose loaded plugins to avoid multiple requests to PluginServlet |
| ENTESB-20016 | Fuse Console - Allow the possibility to set label at the hawtio CR |
| ENTESB-20592 | Certify Fuse 7 on OpenJDK 17 before ELS |
| ENTESB-20667 | operators.openshift.io/valid-subscription annotation for operator metadata bundles |
| ENTESB-20714 | ensure all CXF tests passed with JDK17 |
| ENTESB-20830 | Certify Fuse 7 on RHEL 9 |
| ENTESB-20953 | Upgrade to EAP-7.4.10.GA-redhat-00002 |

8.2. COMPONENT UPGRADES IN FUSE 7.12

The following table lists the component upgrades in Fuse 7.12.

Table 8.1. Fuse 7.12 Component Upgrades

| Issue | Description |
|------------------------------|---|
| ENTESB-20648 | Upgrade Spring Boot to 2.7.12 |
| ENTESB-20849 | Align camel test dependencies to be compatible with JDK17 |
| ENTESB-21063 | Align to kafka-clients v3 |

8.3. BUGS RESOLVED IN FUSE 7.12

The following tables list the resolved bugs in Fuse 7.12.

Table 8.2. Fuse 7.12 Resolved Bugs

| Issue | Description |
|------------------------------|--|
| ENTESB-8337 | Offline repository contains org.jboss.fuse.fis.archetypes group name artifacts |
| ENTESB-12949 | Next button disabled in SQS step creation until I change the autopopulated queue value |
| ENTESB-13046 | Restore using operator binary not working as expected |
| ENTESB-13366 | Operator instructions unclear and secret create steps are not easy to debug |
| ENTESB-13966 | Discovery of deployed integration API seems disabled but not really |
| ENTESB-14552 | support for multicast queue |
| ENTESB-17394 | Error exclamation marks doesn't show error message |
| ENTESB-17404 | Build leveldb-jni for x86 |
| ENTESB-17888 | validation error when connecting to an https endpoint |
| ENTESB-18042 | Failed to watch errors printed in the operator logs |
| ENTESB-18364 | Hawtio - CSP issues when using Hawtio with Keycloak |
| ENTESB-19351 | FIPS on OCP - Jolokia agent doesn't start due to unsupported security encoding |
| ENTESB-19352 | FIPS on OCP - karaf-maven-plugin assembly goal fails to unsupported security provider |
| ENTESB-19745 | Quickstart spring-boot-camel-amq integrations tests references old AMQ Broker version |
| ENTESB-19757 | Provide a source container image for apicurito |
| ENTESB-19956 | [Syndesis] CVE-2022-24785 Moment.js: Path traversal in moment.locale [fuse-7] |
| ENTESB-19986 | Fuse hawtio includes HTTPClient 3.1 - CVE-2012-5783 |
| ENTESB-20096 | AMQ6 image - V2 schema 1 manifest digest are no longer supported for image pulls |
| ENTESB-20175 | Missing dataformats fhir-json/fhir-xml/xml-json in runtime specific catalogs |

| Issue | Description |
|------------------------------|--|
| ENTESB-20177 | Send correct UMB messages for container builds |
| ENTESB-20404 | Camel http4 producer encodes array data to the http uri parameter as comma separated instead of multi-values parameters |
| ENTESB-20485 | CVE-2022-42920 apache-bcel: Apache-Commons-BCEL: arbitrary bytecode produced via out-of-bounds writing [fuse-7] |
| ENTESB-20595 | Backport request for ENTMQCL-2977 to Fuse 7.11.x |
| ENTESB-20596 | CVE-2022-41940 engine.io: Specially crafted HTTP request can trigger an uncaught exception [fuse-7] |
| ENTESB-20598 | Incomplete fix of CVE-2020-13956 |
| ENTESB-20618 | CVE-2022-41881 codec-haproxy: HAProxyMessageDecoder Stack Exhaustion DoS [fuse-7] |
| ENTESB-20619 | CVE-2022-41854 dev-java-snakeyaml: dev-java/snakeyaml: DoS via stack overflow [fuse-7] |
| ENTESB-20626 | CVE-2022-40146 batik: Server-Side Request Forgery (SSRF) vulnerability [fuse-7] |
| ENTESB-20627 | CVE-2022-38398 batik: Server-Side Request Forgery [fuse-7] |
| ENTESB-20628 | CVE-2022-38648 batik: Server-Side Request Forgery [fuse-7] |
| ENTESB-20630 | CVE-2022-46364 CXF: Apache CXF: SSRF Vulnerability [fuse-7] |
| ENTESB-20632 | CVE-2022-46363 CXF: Apache CXF: directory listing / code exfiltration [fuse-7] |
| ENTESB-20637 | CVE-2022-4492 undertow: Server identity in https connection is not checked by the undertow client [fuse-7] |
| ENTESB-20641 | CVE-2022-41946 jdbc-postgresql: postgresql-jdbc: Information leak of prepared statement data due to insecure temporary file permissions [fuse-7] |
| ENTESB-20663 | Errors during Karaf startup with jdk17 |
| ENTESB-20664 | Errors during EAP startup with jdk17 |
| ENTESB-20672 | CVE-2022-45143 tomcat: JsonErrorReportValve injection [fuse-7] |

| Issue | Description |
|------------------------------|---|
| ENTESB-20690 | CVE-2022-36437 hazelcast: Hazelcast connection caching [fuse-7] |
| ENTESB-20693 | Review patch-maven-plugin → karaf-maven-plugin communication |
| ENTESB-20696 | A custom fuse console route doesn't work. |
| ENTESB-20697 | AutomaticRecovery from RabbitMQ Connection Factory is always creating a new connection |
| ENTESB-20701 | fuse-patch may incorrectly report that a patch has already been applied |
| ENTESB-20702 | netty4-http forwards a bad response (exception + http code 200) |
| ENTESB-20710 | CXF test errors after upgrading to Karaf 4.4 and Pax Web 8 |
| ENTESB-20711 | Any issue with camel-aws 2.23 component with TLS 1.3 in Fuse 7.11 ? |
| ENTESB-20712 | Camel test errors after upgrading to Karaf 4.4 and Pax Web 8 |
| ENTESB-20720 | Multicast not returning aggregated |
| ENTESB-20726 | Hazelcast upgrade seems to break JCache Integration |
| ENTESB-20741 | Wrong javax/mail/mail version used in fuse projects. |
| ENTESB-20742 | Wrong log4j-slf4j18-impl version is used fuse projects. |
| ENTESB-20754 | [Hawtio] Can't login in Karaf |
| ENTESB-20826 | CVE-2022-41966 xstream: Denial of Service by injecting recursive collections or maps based on element's hash values raising a stack overflow [fuse-7] |
| ENTESB-20828 | cxfr - server transport isn't up properly |
| ENTESB-20829 | [Karaf] JCE cannot authenticate the provider BC |
| ENTESB-20831 | Use groupified API versions in json files |
| ENTESB-20835 | Karaf pax web - OPTIONS methods not exposed |
| ENTESB-20836 | Hibernate fuse version clashes with spring boot |
| ENTESB-20839 | [Karaf] JMX ACL MBean authentication problem |

| Issue | Description |
|------------------------------|--|
| ENTESB-20840 | [Karaf] 10 features cannot be installed |
| ENTESB-20841 | Fuse archetype Spring Boot properties in SB1 format |
| ENTESB-20842 | camel-master component is unable to load cluster service |
| ENTESB-20845 | CVE-2023-1108 undertow: Infinite loop in SslConduit during close [fuse-7] |
| ENTESB-20847 | [Karaf] Jasypt encryption problem JDK 17 and RHEL8-FIPS |
| ENTESB-20850 | [Standalone] No response messages via fuse client |
| ENTESB-20851 | [Standalone] Colorised commands in history |
| ENTESB-20853 | [Fuse on Openshift] - Wrong Docker image reference in Quickstarts |
| ENTESB-20854 | [Fuse on Openshift] - Application templates - No tag "1.12" with image streams in fis-image-streams.json |
| ENTESB-20855 | [Fuse on Openshift] - Wrong WILDFLY version in EAP images JDK8/11 |
| ENTESB-20857 | [Fuse on Openshift] - Application templates - Templates filled with old 7.11 references |
| ENTESB-20859 | [Patching] Unable to patch 7.11 to 7.12 |
| ENTESB-20862 | [karaf FoO] unable to use client into the POD |
| ENTESB-20869 | CVE-2023-20860 springframework: Security Bypass With Un-Prefixed Double Wildcard Pattern [fuse-7] |
| ENTESB-20870 | CVE-2023-20861 springframework: Spring Expression DoS Vulnerability [fuse-7] |
| ENTESB-20871 | Camel 2.23 tests do not support jdk17 |
| ENTESB-20872 | Wildfly Camel 5.10 tests do not support jdk17 |
| ENTESB-20873 | CXF 3.3.6 tests do not support jdk17 |
| ENTESB-20950 | [Karaf] Doesn't install features |
| ENTESB-20951 | Camel Mail Component doesn't use host/port information from session URI parameter |

| Issue | Description |
|------------------------------|---|
| ENTESB-20956 | CVE-2022-4492, ensure that Syndesis is using fixed undertow |
| ENTESB-20957 | CVE-2023-1108 undertow: Infinite loop in SslConduit during close (fuse online) |
| ENTESB-20958 | CVE-2022-41704 batik: Apache XML Graphics Batik vulnerable to code execution via SVG [fuse-7] |
| ENTESB-20959 | CVE-2022-42890 batik: Untrusted code execution in Apache XML Graphics Batik [fuse-7] |
| ENTESB-20960 | CVE-2023-22602 shiro-core: shiro: Authentication bypass through a specially crafted HTTP request [fuse-7] |
| ENTESB-20961 | [Fuse On Openshift] QS spring-boot-camel-amq contains a removed image |
| ENTESB-20963 | [Fuse On Openshift] QS Spring-Boot Camel Rest SQL reports wrong deployment step in README |
| ENTESB-20964 | [Fuse On Openshift] Adjust Pod metering label rhs.prod_ver formatting |
| ENTESB-20967 | [Fuse on Openshift] QS Spring-Boot Camel Config fails on Spring Cloud due to SB upgrade |
| ENTESB-20966 | Unable to install karaf features separately |
| ENTESB-20968 | [Fuse On Openshift] QS Spring-Boot Camel Rest SQL throws bad SQL grammar exception |
| ENTESB-20969 | [Fuse On Openshift] QS Spring-Boot Camel XA throws bad SQL grammar exception on PostgreSQL connection |
| ENTESB-20971 | Hawtio console metrics shows free memory instead of used |
| ENTESB-21045 | Pax-web-jetty features cannot be installed |
| ENTESB-21046 | [Fuse standalone] Exception in log jdk11 and jdk17 |
| ENTESB-21047 | CVE-2023-20860, ensure that Syndesis is using fixed springframework |
| ENTESB-21048 | Cannot install CVE patch on top of 7.12 |
| ENTESB-21049 | CVE-2022-41854, ensure that Syndesis is using fixed snakeyaml |

| Issue | Description |
|------------------------------|--|
| ENTESB-21050 | Remove org.apache.tomcat.embed dependencies from cxf-spring-boot-starter-jaxrs |
| ENTESB-21051 | [Fuse On Openshift] QS Spring-Boot Camel-Drools, unable to create Kie Server |
| ENTESB-21053 | [Fuse on Openshift] QS Spring Boot Camel Singleton, app won't start |
| ENTESB-21052 | [Fuse on Openshift] - Karaf - Unable to resolve missing requirement in a cxf-jaxrs application |
| ENTESB-21056 | CVE-2023-20861, ensure that Syndesis is using fixed springframework |
| ENTESB-21057 | CVE-2022-41946, ensure that Syndesis is using fixed jdbc-postgresql |
| ENTESB-21058 | Karaf, some bundle versions are not inline with versions specified in karaf-bom |
| ENTESB-21059 | Memory leak in pax-url-aether |
| ENTESB-21061 | CXF 3.3.6 downstream failures |
| ENTESB-21704 | CVE-2023-20863 springframework: Spring Expression DoS Vulnerability [fuse-7] |
| ENTESB-21158 | Unattended Jolokia Queries Not Working When Keycloak is Integrated for Access Control |
| ENTESB-21161 | [Offliner] Files cannot be downloaded using offliner manifest file |
| ENTESB-21162 | [Offliner] Missing artifacts |
| ENTESB-21163 | Apicurito pods contain metering labels with incorrect values |
| ENTESB-21168 | CVE-2023-1370 json-smart: Uncontrolled Resource Consumption vulnerability in json-smart (Resource Exhaustion) [fuse-7] |
| ENTESB-21272 | [Fuse on Openshift] Wrong version in Quickstart BOM |
| ENTESB-21273 | Remove or refactor non-working quickstart spring-boot-camel-soap-rest-bridge |
| ENTESB-21274 | Wildfly camel 5.10.0 downstream failure |

| Issue | Description |
|------------------------------|---|
| ENTESB-21304 | [Fuse on Openshift] - Illegal access on java.xml module using Karaf, jaxws and JDK17, because xerces packages are not exposed |
| ENTESB-21309 | [Fuse on Openshift] - In camel-jdbc on Karaf, can't retrieve a column from the body exchange |
| ENTESB-21310 | Camel-Velocity: Deprecation warnings |
| ENTESB-21311 | SpringFramework caches a missed TypeConverter and user can not clean it |
| ENTESB-21316 | [Fuse On Openshift] - Dismiss/Remove RHOSAK Quickstarts |
| ENTESB-21319 | CVE-2022-31692 spring-security: Authorization rules can be bypassed via forward or include dispatcher types in Spring Security [fuse-7] |
| ENTESB-21322 | Invalid qualifier for Karaf bundle |
| ENTESB-21332 | CVE-2023-20883 spring-boot: Spring Boot Welcome Page DoS Vulnerability [fuse-7] |
| ENTESB-21335 | patch-maven-plugin doesn't work with Maven 3.9 |
| ENTESB-21412 | Missing refs/tags on GitHub |
| ENTESB-21415 | [Fuse Standalone] Camel-chunk feature missing dependency |
| ENTESB-21417 | CXF 3.3.6 downstream failures |
| ENTESB-21418 | CVE-2023-1370, ensure that Syndesis is using fixed json-smart |
| ENTESB-21419 | [Karaf] Jasypt encryption problem JDK 17 and RHEL8-FIPS |
| ENTESB-21421 | Camel health check behaviour change on Spring Boot runtime |

8.4. BUGS RESOLVED IN FUSE 7.12.1

The following tables list the resolved bugs in Fuse 7.12.1.

Table 8.3. Fuse 7.12.1 Resolved Bugs

| Issue | Description |
|------------------------------|---|
| ENTESB-21742 | New Fuse Console deployments don't work after yearly "openshift-service-serving-signer" certificate rotation. |

| Issue | Description |
|--------------------------------|--|
| ENTESB-21757 | [JDG-4351][JBMAR-235] camel-infinispan requires jboss-marshalling update from 2.0.9.Final to 2.0.11.Final onwards |
| ENTESB-21776 | Fuse on Openshift image uses very old jmx_prometheus_javaagent.jar |
| ENTESB-21858 | Karaf won't start when using JDK 11.0.20 |
| ENTESB-21878 | NullPointerException when logging is at WARN level |
| ENTESB-21881 | Problem using -Dpatch for patch-maven-plugin with Maven 3.9 |
| ENTESB-22087 | Cannot install patch 7.12.1 on top of 7.12 |
| ENTESB-21763 | camel-http4 with toD does not work on Karaf |
| ENTESB-21865 | pollEnrich files component behavior change between 6.3 and 7.11 |
| CVE-2023-46604 | CVE-2023-46604 activemq-openwire: OpenWire Module: Unbounded deserialization causes ActiveMQ to be vulnerable to a remote code execution (RCE) attack [fuse-7] |
| CVE-2023-40167 | CVE-2023-40167 jetty-http: jetty: Improper validation of HTTP/1 content-length [fuse-7] |
| CVE-2023-3223 | CVE-2023-3223 undertow: OutOfMemoryError due to @MultipartConfig handling [fuse-7] |
| CVE-2023-36479 | CVE-2023-36479 jetty-servlets: jetty: Improper addition of quotation marks to user inputs in CgiServlet [fuse-7] |
| CVE-2023-39410 | CVE-2023-39410 avro: apache-avro: Apache Avro Java SDK: Memory when deserializing untrusted data in Avro Java SDK [fuse-7] |
| CVE-2023-34034 | CVE-2023-34034 spring-security: spring-security-webflux: path wildcard leads to security bypass [fuse-7] |
| CVE-2023-44487 | CVE-2023-44487 undertow: HTTP/2: Multiple HTTP/2 enabled web servers are vulnerable to a DDoS attack (Rapid Reset Attack) [fuse-7] |
| CVE-2023-36478 | CVE-2023-36478 http2-hpack: jetty: hpack header values cause denial of service in http/2 [fuse-7] |
| CVE-2023-41900 | CVE-2023-41900 jetty-openid: jetty: OpenId Revoked authentication allows one request [fuse-7] |

