



Migration Toolkit for Runtimes 1.2

Release Notes

New features, known issues, and resolved issues

Migration Toolkit for Runtimes 1.2 Release Notes

New features, known issues, and resolved issues

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

This document describes new features, known issues, and resolved issues for the Migration Toolkit for Runtimes.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE	3
CHAPTER 1. INTRODUCTION	4
CHAPTER 2. MTR 1.2.7	5
2.1. KNOWN ISSUES	5
2.2. RESOLVED ISSUES	5
CHAPTER 3. MTR 1.2.6	6
3.1. KNOWN ISSUES	6
3.2. RESOLVED ISSUES	6
CHAPTER 4. MTR 1.2.5	8
4.1. NEW FEATURES	8
4.2. KNOWN ISSUES	8
4.3. RESOLVED ISSUES	8
CHAPTER 5. MTR 1.2.4	9
5.1. NEW FEATURES	9
5.2. KNOWN ISSUES	9
5.3. RESOLVED ISSUES	9
CHAPTER 6. MTR 1.2.3	10
6.1. NEW FEATURES	10
6.2. KNOWN ISSUES	10
6.3. RESOLVED ISSUES	10
CHAPTER 7. MTR 1.2.2	11
7.1. KNOWN ISSUES	11
7.2. RESOLVED ISSUES	11
CHAPTER 8. MTR 1.2.1	12
8.1. KNOWN ISSUES	12
8.2. RESOLVED ISSUES	12
CHAPTER 9. MTR 1.2.0	13
9.1. NEW FEATURES	13
9.1.1. New rulesets and targets	13
9.2. KNOWN ISSUES	13
9.3. RESOLVED ISSUES	13

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. INTRODUCTION



MIGRATION TOOLKIT FOR RUNTIMES PRODUCT WILL BE END OF LIFE ON SEPTEMBER 30TH, 2024

All customers using this product should start their transition to [Migration Toolkit for Applications](#).

Migration Toolkit for Applications is fully backwards compatible with all features and rulesets available in Migration Toolkit for Runtimes and will be maintained in the long term.

Migration Toolkit for Runtimes (MTR) provides an extensible and customizable rule-based tool that simplifies the migration and modernization of Java applications, such as migrating JBoss Enterprise Application Platform (EAP) 7 to 8 or migrating from any other application server towards EAP at scale. MTR provides the same migration solution as provided in the Migration Toolkit for Applications 5 releases.

These release notes cover all Z-stream releases of MTR 1.2 with the most recent release listed first.

CHAPTER 2. MTR 1.2.7

2.1. KNOWN ISSUES

The following known issues are in the MTR 1.2.7 release:

For a complete list of all known issues, see the list of [MTR 1.2.7 known issues](#) in Jira.

2.2. RESOLVED ISSUES

MTR 1.2.7 has the following resolved issues:

MTR 1.2.0 fails with the Exception

java.lang.ClassNotFoundException:org.eclipse.text.edits.MalformedTreeException

In earlier versions of MTR 1.2.z, when migrating an Application from JBoss Enterprise Application Platform (EAP) 7 to EAP 8, there could be a failure with the following

java.lang.ClassNotFoundException:

```
java.lang.ClassNotFoundException: org.eclipse.text.edits.MalformedTreeException from [Module
"org.jboss.windup.ast.windup-java-ast:6.3.1.Final-redhat-00002_67e96e90-d3bc-44fe-8fc8-
ac2abdeacc58" from AddonModuleLoader]
```

This issue has been resolved in MTR 1.2.7. ([WINDUP-4200](#))

CVE-2022-36033: org.jsoup/jsoup: The jsoup cleaner may incorrectly sanitize crafted XSS attempts if SafeList.preserveRelativeLinks is enabled

A flaw was discovered in **jsoup**, which is a Java HTML parser, built for HTML editing, cleaning, scraping, and cross-site scripting (XSS) safety.

An issue in **jsoup** could incorrectly sanitize HTML, including javascript: URL expressions, which could allow XSS attacks when a reader subsequently clicks that link. If the non-default `SafeList.preserveRelativeLinks` option is enabled, HTML, including javascript: URLs crafted with control characters, will not be sanitized. Users are recommended to upgrade to MTR 1.2.7, which resolves this issue.

For more details, see ([2022-36033](#)).

For a complete list of all issues resolved in this release, see the list of [MTR 1.2.7 resolved issues](#) in Jira.

CHAPTER 3. MTR 1.2.6

3.1. KNOWN ISSUES

The following known issues are in the MTR 1.2.6 release:

Unable to migrate an application to MTR due to a **SEVERE [org.jboss.windup.web.services.messaging.PackageDiscoveryMDB]** error

When uploading files for analysis, the server log would return a **SEVERE [org.jboss.windup.web.services.messaging.PackageDiscoveryMDB]** error. This error is caused by a **null: java.lang.NullPointerException.** ([WINDUP-4189](#))

For a complete list of all known issues, see the list of [MTR 1.2.6 known issues](#) in Jira.

3.2. RESOLVED ISSUES

MTR 1.2.6 has the following resolved issues:

CVE-2024-1132: org.keycloak-keycloak-parent: keycloak path transversal in redirection validation

A flaw was discovered in Keycloak, where it does not properly validate URLs included in a redirect. This flaw could allow an attacker to construct a malicious request to bypass validation, access other URLs and sensitive information within the domain, or conduct further attacks. Users are recommended to upgrade to MTR 1.2.6, which resolves this issue.

For more details, see ([CVE-2024-1132](#)).

CVE-2023-45857: Axios 1.5 exposes confidential data stored in cookies

A flaw was discovered in Axios 1.5.1 that accidentally revealed the confidential **XSRF-TOKEN**, stored in cookies, by including it in the HTTP header **X-XSRF-TOKEN** for every request made to any host, thereby allowing attackers to view sensitive information. Users are recommended to upgrade to MTR 1.2.6, which resolves this issue.

For more details, see ([CVE-2023-45857](#)).

CVE-2024-28849: follow-redirects package clears authorization headers

A flaw was discovered in the **follow-redirects** package, which clears authorization headers, but it fails to clear the **proxy-authentication** headers. This flaw could lead to credential leakage, which could have a high impact on data confidentiality. Users are recommended to upgrade to MTR 1.2.6, which resolves this issue.

For more details, see ([CVE-2024-28849](#)).

CVE-2024-29131: Out-of-bounds Write vulnerability in Apache Commons Configuration

A vulnerability was found in Apache Commons-Configuration2, where a Stack Overflow Error can occur when adding a property in the **AbstractListDelimiterHandler.flattenIterator()** method. This issue could allow an attacker to corrupt memory or execute a denial of service (DoS) attack by crafting a malicious property that triggers an out-of-bounds write issue when processed by the vulnerable method. Users are recommended to upgrade to MTR 1.2.6, which resolves this issue.

For more details, see ([CVE-2024-29131](#))

CVE-2024-29133: Out-of-bounds Write vulnerability in Apache Commons Configuration

A vulnerability was found in Apache Commons-Configuration2, where a Stack Overflow Error occurs when calling the **ListDelimiterHandler.flatten(Object, int)** method with a cyclical object tree. This issue could allow an attacker to trigger an out-of-bounds write that could lead to memory corruption or cause a denial of service (DoS) attack. Users are recommended to upgrade to MTR 1.2.6, which resolves this issue.

For more details, see [\(CVE-2024-29133\)](#)

CVE-2024-29180: webpack-dev-middleware lack of URL validation may lead to a file leak

A flaw was found in the **webpack-dev-middleware** package, where it failed to validate the supplied URL address sufficiently before returning local files. This flaw allows an attacker to craft URLs to return arbitrary local files from the developer's machine. The lack of normalization before calling the middleware also allows the attacker to perform path traversal attacks on the target environment. Users are recommended to upgrade to MTR 1.2.6, which resolves this issue.

For more details, see [\(CVE-2024-29180\)](#)

CVE-2023-4639: org.keycloak-keycloak-parent undertow Cookie Smuggling and Spoofing

A flaw was found in Undertow, which incorrectly parses cookies with certain value-delimiting characters in incoming requests. This vulnerability has the potential to enable an attacker to construct a cookie value to intercept **HttpOnly** cookie values or spoof arbitrary additional cookie values, resulting in unauthorized data access or modification. Users are recommended to upgrade to MTR 1.2.6, which resolves this issue.

For more details, see [\(CVE-2023-4639\)](#).

CVE-2023-36479: com.google.guava-guava-parent improper addition of quotation marks to user inputs in Jetty CGI Servlet

A flaw was found in Jetty's **org.eclipse.jetty.servlets.CGI** Servlet, which permits incorrect command execution in specific circumstances, such as requests with certain characters in requested filenames. This issue could allow an attacker to run permitted commands besides the ones requested. Users are recommended to upgrade to MTR 1.2.6, which resolves this issue.

For more details, see [\(CVE-2023-36479\)](#).

CVE-2023-26364: css-tools improper input validation causes denial of service

A flaw was found in **@adobe/css-tools**, which could potentially lead to a minor denial of service (DoS) when parsing CSS. User interaction and privileges are not required to jeopardize an environment. Users are recommended to upgrade to MTR 1.2.6, which resolves this issue.

For more details, see [\(CVE-2023-26364\)](#).

CVE-2023-48631: css-tools: regular expression denial of service

A flaw was found in **@adobe/css-tools**, which could lead to a regular expression denial of service (ReDoS) when attempting to parse CSS. Users are recommended to upgrade to MTR 1.2.6, which resolves this issue.

For more details, see [\(CVE-2023-48631\)](#).

For a complete list of all issues resolved in this release, see the list of [MTR 1.2.6 resolved issues](#) in Jira.

CHAPTER 4. MTR 1.2.5

4.1. NEW FEATURES

Migration Toolkit for Runtimes (MTR) 1.2.5 has the following new features:

New ruleset for MicroProfile metrics replaces old ruleset

A new ruleset for MicroProfile (MP) metrics replaces the old ruleset. ([WINDUPRULE-1043](#))

New ruleset for MicroProfile OpenTracing replaces the old ruleset

A new ruleset for MicroProfile (MP) OpenTracing replaces the old ruleset. ([WINDUPRULE-1044](#))

4.2. KNOWN ISSUES

There are no major known issues in this Migration Toolkit for Runtimes (MTR) 1.2.5 release.

For a complete list of all known issues, see the list of [MTR 1.2.5 known issues](#) in Jira.

4.3. RESOLVED ISSUES

Migration Toolkit for Runtimes (MTR) 1.2.5 resolves the following issues:

CVE-2024-25710 commons-compress: Denial of service caused by an infinite loop

A loop with an unreachable exit condition, meaning an Infinite Loop, vulnerability, was found in Apache Commons Compress. This issue could have led to a denial of service. This issue affects Apache Commons Compress: from 1.3 through 1.25.0. Users are recommended to upgrade to MTR 1.2.5, which resolves this issue.

For more details, see ([CVE-2024-25710](#)).

CVE-2024-26308 commons-compress: OutOfMemoryError

An allocation of resources without limits or throttling vulnerability was found in Apache Commons Compress. This issue could lead to an out-of-memory error (OOM). This issue affects Apache Commons Compress, from 1.21 to 1.26. Users are recommended to upgrade to MTR 1.2.5, which resolves this issue.

For more details, see ([CVE-2024-26308](#)).

CVE-2024-1300: A vulnerability in the Eclipse Vert.x toolkit causes a memory leak in TCP servers configured with TLS and SNI support

A vulnerability in the Eclipse Vert.x toolkit causes a memory leak in Transmission Control Protocol (TCP) servers configured with TLS and SNI support. When processing an unknown Server Name Indication (SNI) server name assigned the default certificate instead of a mapped certificate, the Secure Sockets Layer (SSL) context is erroneously cached in the server name map, leading to memory exhaustion. This affects only TLS servers with SNI enabled. Users are recommended to upgrade to MTR 1.2.5, which resolves this issue.

For more details, see ([CVE-2024-1300](#)).

For a complete list of all issues resolved in this release, see the list of [MTR 1.2.5 resolved issues](#) in Jira.

CHAPTER 5. MTR 1.2.4

5.1. NEW FEATURES

This section describes the new features of the Migration Toolkit for Runtimes (MTR) 1.2.4:

1. New rules support the migration of Red Hat JBoss Enterprise Application Platform (EAP 7) to EAP 8.
2. New rules support the migration of Jakarta EE applications to Quarkus.

5.2. KNOWN ISSUES

For a complete list of all known issues, see the list of [MTR 1.2.4 known issues](#) in Jira.

5.3. RESOLVED ISSUES

CVE-2023-26159: follow-redirects package before 1.15.4 are vulnerable to Improper Input Validation

Versions of the **follow-redirects** package before 1.15.4 are vulnerable to Improper Input Validation. This vulnerability is due to the improper handling of URLs by the **url.parse()** function. When a new URL returns an error, it can be manipulated to misinterpret the hostname. An attacker could exploit this weakness to redirect traffic to a malicious site, potentially leading to information disclosure, phishing attacks, or other security breaches.

For more details, see [\(CVE-2023-26159\)](#).

CVE-2022-25883: Regular Expression Denial of Service (ReDoS) vulnerability was discovered in the node-semver package

Versions of the **semver** npm package before 7.5.2 are vulnerable to Regular Expression Denial of Service (ReDoS). This ReDoS vulnerability comes from the **new Range** function, when untrusted user data is provided as a range.

For more details, see [\(CVE-2022-25883\)](#).

CVE-2023-26136: tough-cookie package before 4.1.3 are vulnerable to Prototype Pollution

Versions of the **tough-cookie** package before 4.1.3 are vulnerable to Prototype Pollution. This vulnerability is due to improper handling of Cookies when using **CookieJar** in **rejectPublicSuffixes=false** mode. This issue arises from the manner in which the objects are initialized.

For more details, see [\(CVE-2023-26136\)](#).

CVE-2023-35116: jackson-databind before 2.15.2 are vulnerable to Denial of Service or other unspecified impact

Versions of the **jackson-databind** library before 2.15.2 are vulnerable to Denial of Service (DoS) attacks or other unspecified impacts using a crafted object that uses cyclic dependencies.

For more details, see [\(CVE-2023-35116\)](#).

For a complete list of all issues resolved in this release, see the list of [MTR 1.2.4 resolved issues](#) in Jira.

CHAPTER 6. MTR 1.2.3

6.1. NEW FEATURES

This section describes the new features of the Migration Toolkit for Runtimes (MTR) 1.2.3:

1. New rules support for Camel 4.1.
2. New rules support the migration of Java EE applications to Quarkus.

6.2. KNOWN ISSUES

For a complete list of all known issues, see the list of [MTR 1.2.3 known issues](#) in Jira.

6.3. RESOLVED ISSUES

CVE-2023-1436 org.keycloak-keycloak-parent: Jettison: Uncontrolled Recursion in JSONArray

A flaw in **Jettison**, which was utilized by MTR, triggers an infinite recursion when constructing a **JSONArray** from a Collection where one of the elements self-references. This flaw throws a **StackOverflowError** exception. ([WINDUP-3772](#))

For more details, see [CVE-2023-1436](#)

For a complete list of all issues resolved in this release, see the list of [MTR 1.2.3 resolved issues](#) in Jira.

CHAPTER 7. MTR 1.2.2

7.1. KNOWN ISSUES

For a complete list of all known issues, see the list of [MTR 1.2.2 known issues](#) in Jira.

7.2. RESOLVED ISSUES

CVE-2023-44487 netty-codec-http2: HTTP/2: Multiple HTTP/2 enabled web servers are vulnerable to a DDoS attack (Rapid Reset Attack)

A flaw was found in handling multiplexed streams in the HTTP/2 protocol, which was utilized by Migration Toolkit for Runtimes (MTR). A client could repeatedly make a request for a new multiplex stream and immediately send an **RST_STREAM** frame to cancel it. This creates additional workload for the server in terms of setting up and dismantling streams, while avoiding any server-side limitations on the maximum number of active streams per connection, resulting in a denial of service due to server resource consumption. ([WINDUP-4072](#))

For more details, see ([CVE-2023-44487](#))

CVE-2023-37460 plexus-archiver: Arbitrary File Creation in AbstractUnArchiver

A flaw was found in the Plexus Archiver, which was utilized by MTR. While using **AbstractUnArchiver** for extracting, an archive could lead to arbitrary file creation and possible remote code execution (RCE). This flaw will bypass directory destination verification if an archive with an entry in the destination directory as a symbolic link whose target does not exist. The plexus-archiver is a test scoped artifact so not included in any of the MTR distributions. ([WINDUP-4053](#))

For more details, see ([CVE-2023-37460](#))

EAP 7.3 and EAP 7.4 rules with target EAP 7.0 and above

This MTR release makes a correction to some rules to support migrating to EAP 7.3 and above, to ensure the rules are ignored if the target is EAP 7.2 or below. ([WINDUPRULE-1038](#))

CHAPTER 8. MTR 1.2.1

8.1. KNOWN ISSUES

For a complete list of all known issues, see the list of [MTR 1.2.1 known issues](#) in Jira.

8.2. RESOLVED ISSUES

CVE-2023-44487 netty-codec-http2: HTTP/2

Multiple HTTP/2 enabled web servers are vulnerable to a DDoS attack (Rapid Reset Attack). The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly. ([WINDUP-4056](#))

For a complete list of all issues resolved in this release, see the list of [MTR 1.2.1 resolved issues](#) in Jira.

CHAPTER 9. MTR 1.2.0

9.1. NEW FEATURES

This section describes the new features of the Migration Toolkit for Runtimes (MTR) 1.2.0.

1. Decompile and analysis of applications based on Java 17
2. Rules Override enhancement: A new condition has been added for overriding an existing rule. In addition to matching **rulesetId** and **ruleId**, the target technology in the override ruleset must match one of the targets that the user specified for running the analysis.
3. Eclipse Plugin Java 17 compatibility
4. Upgrade of the Windup Operator: Adopted **Quarkus 2.13.7.Final** and the **Quarkus Operator SDK 4.0.8**

9.1.1. New rulesets and targets

1. OpenJDK 21: Rules to support the upgrading to OpenJDK 21.
2. Red Hat JBoss Web Server 6: Rules to support the upgrade of JWS and Tomcat applications to JWS 6 and Tomcat 10.
3. Camel 4: Comprehensive rulesets supporting upgrade to all Y-stream releases of Camel 3 and Camel 4.
4. More migration rules to support Red Hat JBoss EAP 8 and Hibernate 6.
5. Java/Jakarta EE to Quarkus: New rulesets support migrating Java/Jakarta EE applications to Quarkus 3. These rulesets cover the *quarkification* of the project, along with JAX-RS and CDI technologies. Additional rules that support this migration path are still under development and will be made available in future Z-stream releases.

9.2. KNOWN ISSUES

For a complete list of all known issues, see the list of [MTR 1.2.0 known issues](#) in Jira.

9.3. RESOLVED ISSUES

For a complete list of all issues resolved in this release, see the list of [MTR 1.2.0 resolved issues](#) in Jira.