Migration Toolkit for Runtimes 1.2

发行注记

新功能、已知问题和已解决的问题

Last Updated: 2024-06-13

Migration Toolkit for Runtimes 1.2 发行注记

新功能、已知问题和已解决的问题

法律通告

摘要

本文档描述了 Migration Toolkit for Runtimes 的新功能、已知问题和已解决的问题。

目录

使开源包含更多 3

第 1 章 简介 4

第 2 章 MTR 1.2.6 5
2.1. 已知问题 5
2.2. 已解决的问题 5

第 3 章 MTR 1.2.5 7
3.1. 新功能 7
3.2. 已知问题 7
3.3. 已解决的问题 7

第 4 章 MTR 1.2.4 8
4.1. 新功能 8
4.2. 已知问题 8
4.3. 已解决的问题 8

第 5 章 MTR 1.2.3 9
5.1. 新功能 9
5.2. 已知问题 9
5.3. 已解决的问题 9

第 6 章 MTR 1.2.2 10
6.1. 已知问题 10
6.2. 已解决的问题 10

第 7 章 MTR 1.2.1 11
7.1. 已知问题 11
7.2. 已解决的问题 11

第 8 章 MTR 1.2.0 12
8.1. 新功能 12
8.2. 已知问题 12
8.3. 已解决的问题 12

使开源包含更多

红帽致力于替换我们的代码、文档和 Web 属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于此项工作十分艰巨，这些更改将在即将推出的几个发行版本中逐步实施。有关更多详情，请参阅我们的首席技术官 Chris Wright 提供的消息。

第 1 章 简介

Migration Toolkit for Runtimes (MTR)提供可扩展的可定制规则的工具，可以简化 Java 应用程序的迁移和现代化，如将 JBoss 企业应用平台(EAP) 7 迁移到 8，或大规模从任何其他应用服务器迁移到 EAP。MTR 提供与 Migration Toolkit for Applications 5 版本中提供的相同的迁移解决方案。

本发行注记涵盖了 MTR 1.2 的所有 Z-stream 版本，以及首先列出的最新发行版本。

第 2 章 MTR 1.2.6

2.1. 已知问题

MTR 1.2.6 发行版本中有以下已知问题：

由于 SEVERE [org.jboss.windup.web.services.messaging.PackageDiscoveryMDB] 错误，无法将应用程序迁移到 MTR

在上传文件进行分析时，服务器日志会返回 **SEVERE [org.jboss.windup.web.services.messaging.PackageDiscoveryMDB]** 错误。此错误是由 **null: java.lang.NullPointerException** 导致的。(WINDUP-4189)

有关所有已知问题的完整列表，请参阅 JIRA 中的 MTR 1.2.6 已知问题 列表。

2.2. 已解决的问题

MTR 1.2.6 有以下已解决的问题：

CVE-2024-1132: org.keycloak-keycloak-parent: keycloak 路径转换（在重定向验证中）

Keycloak 中发现了一个安全漏洞，它没有正确验证重定向中包含的 URL。此漏洞允许攻击者构建恶意请求，以绕过验证、访问域中的其他 URL 和敏感信息，或者进行进一步攻击。建议用户升级到 MTR 1.2.6，从而解决了这个问题。

如需了解更多详细信息，请参阅 (CVE-2024-1132)。

CVE-2023-45857: Axios 1.5 会公开存储在 Cookie 中的机密数据

在 Axios 1.5.1 中发现了一个安全漏洞，它意外发现了存储在 Cookie 中的机密 **XSRF-TOKEN**，方法是包括每个对任何主机发出的 HTTP 标头 **X-XSRF-TOKEN**，从而允许攻击者查看敏感信息。建议用户升级到 MTR 1.2.6，从而解决了这个问题。

如需了解更多详细信息，请参阅 (CVE-2023-45857)。

CVE-2024-28849: follow-redirects 软件包清除授权标头

在 **follow-redirects** 软件包中发现了一个安全漏洞，它清除授权标头，但它无法清除 **proxy-authentication** 标头。此漏洞可能会导致凭证泄漏，这可能会对数据保密性产生重大影响。建议用户升级到 MTR 1.2.6，从而解决了这个问题。

如需了解更多详细信息，请参阅 (CVE-2024-28849)

CVE-2024-29131: Apache Commons Configuration 中的超出边界写漏洞

在 Apache Commons-Configuration2 中发现了一个漏洞，在 **AbstractListDelimiterHandler.flattenIterator** （） 方法中添加属性时可能会出现 Stack Overflow Error。此问题可能会使攻击者破坏内存或执行拒绝服务(DoS)攻击，它通过设计一个恶意属性，在通过易受攻击的方法处理时触发越界写入问题。建议用户升级到 MTR 1.2.6，从而解决了这个问题。

如需了解更多详细信息，请参阅 (CVE-2024-29131)

CVE-2024-29133: Apache Commons Configuration 中的超出边界写漏洞

在 Apache Commons-Configuration2 中发现了一个漏洞，其中 Stack Overflow Error 在调用带有 cyclical 对象树的 **ListDelimiterHandler.flatten (Object, int)** 方法时发生。此问题可能会允许攻击者触发越界写入，这可能会导致内存损坏或导致拒绝服务(DoS)附加。建议用户升级到 MTR 1.2.6，从而解决了这个问

题。

如需了解更多详细信息，请参阅 (CVE-2024-29133)

CVE-2024-29180: webpack-dev-middleware 缺少 URL 验证可能会导致文件泄漏

webpack-dev-middleware 软件包中发现了一个安全漏洞，在返回本地文件前无法验证提供的 URL 地址。此漏洞允许攻击者制作 URL 来从开发人员的计算机返回任意本地文件。在调用中间件前缺少规范化还允许攻击者对目标环境执行路径遍历攻击。建议用户升级到 MTR 1.2.6，从而解决了这个问题。

如需了解更多详细信息，请参阅 (CVE-2024-29180)

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

Undertow 中发现了一个安全漏洞，它错误地解析带有传入请求中的特定值限制字符的 Cookie。此漏洞可以让攻击者构建 Cookie 值，以截获 **HttpOnly** cookie 值或欺骗任意 Cookie 值，从而导致未经授权的数据访问或修改。建议用户升级到 MTR 1.2.6，从而解决了这个问题。

如需了解更多详细信息，请参阅 (CVE-2023-4639)。

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

Jetty 的 **org.eclipse.jetty.servlets.CGI** Servlet 中发现了一个安全漏洞，它允许在特定情况下执行不正确的命令，如在请求的文件名中带有某些字符的请求。此问题可能会允许攻击者在请求的命令之外运行允许的命令。建议用户升级到 MTR 1.2.6，从而解决了这个问题。

如需了解更多详细信息，请参阅 (CVE-2023-36479)

CVE-2023-26364: css-tools 不正确的输入验证会导致拒绝服务

在 **@adobe/css-tools** 中发现了一个安全漏洞，这可能会在解析 CSS 时导致拒绝服务(DoS)。强制环境不需要用户交互和特权。建议用户升级到 MTR 1.2.6，从而解决了这个问题。

如需了解更多详细信息，请参阅 (CVE-2023-26364)。

CVE-2023-48631: css-tools: 正则表达式拒绝服务

在 **@adobe/css-tools** 中发现了一个安全漏洞，在尝试解析 CSS 时可能会导致正则表达式拒绝服务(ReDoS)。建议用户升级到 MTR 1.2.6，从而解决了这个问题。

如需了解更多详细信息，请参阅 (CVE-2023-48631)。

有关本发行版本中解决的所有问题的完整列表，请参阅 JIRA 中的 MTR 1.2.6 解决的问题 列表。

第 3 章 MTR 1.2.5

3.1. 新功能

Migration Toolkit for Runtimes (MTR) 1.2.5 具有以下新功能：

MicroProfile 指标的新规则集取代了旧的规则集

MicroProfile (MP)指标的新规则集取代了旧的规则集。(WINDUPRULE-1043)

MicroProfile OpenTracing 的新规则集取代了旧的规则集

MicroProfile (MP) OpenTracing 的新规则集取代了旧的规则集。(WINDUPRULE-1044)

3.2. 已知问题

此 Migration Toolkit for Runtimes (MTR) 1.2.5 发行版本中没有主要已知问题。

有关所有已知问题的完整列表，请参阅 JIRA 中的 MTR 1.2.5 已知问题 列表。

3.3. 已解决的问题

Migration Toolkit for Runtimes (MTR) 1.2.5 解决了以下问题：

CVE-2024-25710 commons-compress：由无限循环导致的服务拒绝

在 Apache Common Compress 中发现了一个带有无法访问的退出条件的循环，即 Infinite Loop (Loop) 漏洞。此问题可能会导致拒绝服务。此问题会影响 Apache Commons Compress: from 1.3 到 1.25.0。建议用户升级到 MTR 1.2.5，这可以解决这个问题。

如需了解更多详细信息，请参阅 (CVE-2024-25710)。

CVE-2024-26308 commons-compress: OutOfMemoryError

在 Apache Commons Compress 中发现没有限制或节流的漏洞的资源分配。此问题可能会导致内存不足错误(OOM)。此问题会影响 Apache Commons Compress, from 1.21 到 1.26。建议用户升级到 MTR 1.2.5，这可以解决这个问题。

如需了解更多详细信息，请参阅 (CVE-2024-26308)。

Eclipse Vert.x 工具包中的 CVE-2024-1300: A 漏洞会导致使用 TLS 和 SNI 配置的 TCP 服务器中的内存泄漏

Eclipse Vert.x 工具包中的漏洞会导致使用 TLS 和 SNI 支持的传输控制协议(TCP)服务器出现内存泄漏。当处理一个未知的 Server Name Indication (SNI)服务器名称而不是映射的证书时，安全套接字层(SSL)上下文会错误地缓存在服务器名称映射中，从而导致内存耗尽。这只会影响启用了 SNI 的 TLS 服务器。建议用户升级到 MTR 1.2.5，这可以解决这个问题。

如需了解更多详细信息，请参阅 (CVE-2024-1300)。

有关本发行版本中解决的所有问题的完整列表，请参阅 JIRA 中的 MTR 1.2.5 解决的问题 列表。

第 4 章 MTR 1.2.4

4.1. 新功能

本节论述了 Migration Toolkit for Runtimes (MTR) 1.2.4 的新功能：

1. 新规则支持将 Red Hat JBoss Enterprise Application Platform (EAP 7)迁移到 EAP 8。
2. 新规则支持将 Jakarta EE 应用程序迁移到 Quarkus。

4.2. 已知问题

有关所有已知问题的完整列表，请参阅 JIRA 中的 MTR 1.2.4 已知问题 列表。

4.3. 已解决的问题

CVE-2023-26159: 在 1.15.4 之前 的后续重定向 软件包会受到 Improper Input Validation 的影响

1.15.4 之前 **的后续重定向** 软件包版本容易受到 Improper 输入验证的影响。此漏洞是由于 **url.parse** （）函数处理 URL 不正确。当新 URL 返回错误时，可以对其进行操作来误解主机名。攻击者可能会利用这种弱点来将流量重定向到恶意网站，从而可能导致信息泄露、辨别攻击或其他安全漏洞。

如需了解更多详细信息，请参阅 (CVE-2023-26159)。

CVE-2022-25883: 在 node-semver 软件包中发现了正则表达式服务(ReDoS)漏洞

7.5.2 之前的 **semver** npm 软件包的版本容易受到 Regular Expression Denial Service (ReDoS)的影响。当不受信任的用户数据作为范围提供时，这个 ReDoS 漏洞来自 **新的 Range** 功能。

如需了解更多详细信息，请参阅 (CVE-2022-25883)。

CVE-2023-26136: 在 4.1.3 之前使用 tough-cookie 软件包会受到 Prototype Pollution 的攻击

4.1.3 之前的 **tough-cookie** 软件包的版本容易受到 Prototype Pollution 的攻击。此漏洞是在 **rejectPublicSuffixes=false** 模式下使用 **CookieJar** 时不正确的处理 Cookie。此问题源自初始化对象的方式。

如需了解更多详细信息，请参阅 (CVE-2023-26136)。

CVE-2023-35116: jackson-databind before 2.15.2 会受到 Denial Service 或其他未指定影响的影响

2.15.2 之前 **Jackson-databind** 库版本会受到 Denial Service (DoS)攻击，或使用 cyclic 依赖项的精心设计的对象或其他未指定影响。

如需了解更多详细信息，请参阅 (CVE-2023-35116)。

有关本发行版本中解决的所有问题的完整列表，请参阅 JIRA 中的 MTR 1.2.4 解决的问题 列表。

第 5 章 MTR 1.2.3

5.1. 新功能

本节论述了 Migration Toolkit for Runtimes (MTR) 1.2.3 的新功能：

1. 对 Camel 4.1 的新规则支持。
2. 新规则支持将 Java EE 应用程序迁移到 Quarkus。

5.2. 已知问题

有关所有已知问题的完整列表，请参阅 JIRA 中的 MTR 1.2.3 已知问题 列表。

5.3. 已解决的问题

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

MTR 使用的 **Jettison** 中的一个缺陷，会在构建自引用 项 之一的集合时触发无限递归。此漏洞会抛出一个 **StackOverflowError** 异常。(WINDUP-3772)

如需了解更多详细信息，请参阅 CVE-2023-1436

有关本发行版本中解决的所有问题的完整列表，请参阅 JIRA 中的 MTR 1.2.3 解决的问题 列表。

第 6 章 MTR 1.2.2

6.1. 已知问题

有关所有已知问题的完整列表，请参阅 JIRA 中的 MTR 1.2.2 已知问题 列表。

6.2. 已解决的问题

CVE-2023-44487 netty-codec-http2: HTTP/2: 多 HTTP/2 启用的 Web 服务器容易受到 DDoS 攻击(Rapid Reset Attack)的影响

在处理 HTTP/2 协议中的多路流中发现了一个安全漏洞，它被 Migration Toolkit for Runtimes (MTR)使用。客户端可以重复请求新的多路流，并立即发送 **RST_STREAM** 帧来取消它。这在设置和分离流方面为服务器创建额外的工作负载，同时避免每个连接的最大活跃流数量的服务器端限制，从而导致因为服务器资源消耗而拒绝服务。(WINDUP-4072)

如需了解更多详细信息，请参阅 (CVE-2023-44487)

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

在 Plexus Archiver 中发现了一个安全漏洞，MTR 会使用该归档器。 在使用 **AbstractUnArchiver** 进行提取时，存档可能会导致任意文件创建和可能执行远程代码(RCE)。如果目标目录中带有条目作为目标不存在的符号链接，则此缺陷将绕过目录目的地验证。plexus-archiver 是一个测试范围工件，因此不会包含在任何 MTR 发行版中。(WINDUP-4053)

如需了解更多详细信息，请参阅 (CVE-2023-37460)

EAP 7.3 和 EAP 7.4 规则带有目标 EAP 7.0 及更高版本

此 MTR 发行版本对一些支持迁移到 EAP 7.3 及更高版本的规则进行修正，以确保如果目标是 EAP 7.2 或更高版本，则忽略规则。(WINDUPRULE-1038)

第 7 章 MTR 1.2.1

7.1. 已知问题

有关所有已知问题的完整列表，请参阅 JIRA 中的 MTR 1.2.1 已知问题 列表。

7.2. 已解决的问题

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

启用的多个 HTTP/2 的 Web 服务器容易受到 DDoS 攻击(Rapid Reset Attack)的影响。HTTP/2 协议允许拒绝服务（服务器资源消耗），因为请求可以快速重置许多流。(WINDUP-4056)

有关本发行版本中解决的所有问题的完整列表，请参阅 JIRA 中的 MTR 1.2.1 解决的问题 列表。

第 8 章 MTR 1.2.0

8.1. 新功能

本节论述了 Migration Toolkit for Runtimes (MTR) 1.2.0 的新功能。

1. 根据 Java 17 解编译和分析应用程序
2. 规则覆盖增强： 添加了一个新的条件来覆盖现有规则。除了匹配的 **rulesetId** 和 **ruleId** 外，覆盖规则集中的目标技术必须与用户为运行分析指定的目标之一匹配。
3. Eclipse 插件 Java 17 兼容性
4. Windup Operator 的升级： **Quarkus 2.13.7.Final** 和 **Quarkus Operator SDK 4.0.8**

8.1.1. 新规则集和目标

1. OpenJDK 21：支持升级到 OpenJDK 21 的规则。
2. Red Hat JBoss Web Server 6：支持将 JWS 和 Tomcat 应用程序升级到 JWS 6 和 Tomcat 10 的规则。
3. Camel 4：支持升级到 Camel 3 和 Camel 4 的所有 Y-stream 版本的综合规则集。
4. 支持 Red Hat JBoss EAP 8 和 Hibernate 6 的更多迁移规则。
5. Java/Jakarta EE 到 Quarkus：新规则集支持将 Java/Jakarta EE 应用迁移到 Quarkus 3。这些规则集涵盖了项目的 *定量* 要求，以及 JAX-RS 和 CDI 技术。支持此迁移路径的附加规则仍在开发中，并将在以后的 Z-stream 版本中提供。

8.2. 已知问题

有关所有已知问题的完整列表，请参阅 JIRA 中的 MTR 1.2.0 已知问题列表。

8.3. 已解决的问题

有关本发行版本中解决的所有问题的完整列表，请参阅 JIRA 中的 MTR 1.2.0 解决的问题列表。