Migration Toolkit for Applications 6.2

Release Notes

New features, known issues, and resolved issues

Last Updated: 2024-02-26

Migration Toolkit for Applications 6.2 Release Notes

New features, known issues, and resolved issues

Legal Notice

Abstract

Migration Toolkit for Applications 6.2 accelerates large-scale application modernization efforts across hybrid cloud environments on Red Hat OpenShift. This solution provides insight throughout the adoption process, at both the portfolio and application levels: inventory, assess, analyze, and manage applications for faster migration to OpenShift via the user interface. This document describes new features and improvements, known issues, and resolved issues for the Migration Toolkit for Applications, version 6.2.

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 Applications 6.2 accelerates large-scale application modernization efforts across hybrid cloud environments on Red Hat OpenShift. This solution provides insight throughout the adoption process, at both the portfolio and application levels: inventory, assess, analyze, and manage applications for faster migration to OpenShift via the user interface.

These release notes cover all *z*-stream releases of MTA 6.2 with the most recent release listed first.

CHAPTER 2. MTA 6.2.2

2.1. RESOLVED ISSUES

The following highlighted issues have been resolved in Migration Toolkit for Applications (MTA) version 6.2.2.

CVE-2022-45693: Vulnerability in Jettison

Versions of Jettison before v1.5.2 are vulnerable to a Denial of Service (DoS) caused by a stack-based buffer overflow. By sending a specially crafted request using the map parameter, a remote attacker could exploit this vulnerability to cause a DoS attack. This issue has been resolved in MTA version 6.2.2.

For more details, see (CVE-2022-45693).

CVE-2023-29406: HTTP/1 client does not fully validate the contents of the Host header

Versions of Golang before 1.19.11 are vulnerable to HTTP header injection, caused by improper contents validation of Host header by the HTTP/1 client. A maliciously crafted Host header can inject additional headers or entire requests. In version 1.19.11 Golang, and later, the **HTTP/1** client now refuses to send requests containing an invalid **Request.Host** or **Request.URL.Host** value. This issue has been resolved in MTA version 6.2.2.

For more details, see (CVE-2023-29406).

CVE-2023-29409: Extremely large RSA keys in certificate chains can cause a client/server to expend significant CPU time verifying signatures

Extremely large RSA keys in certificate chains can cause a client/server to expend significant CPU time verifying signatures. A Denial of Service (DoS) vulnerability was found in the Golang Go package, caused by an uncontrolled resource consumption flaw. By persuading a victim to use a specially crafted certificate with large RSA keys, a remote attacker can cause a client/server to expend significant CPU time verifying signatures, resulting in a denial of service condition. This issue has been resolved in MTA version 6.2.2.

For more details, see (CVE-2023-29409).

CVE-2022-1962: Uncontrolled recursion in the Parse functions in go/parser

In versions of Golang, before 1.17.12 and 1.18.4, a flaw was found in the standard library **go/parser**, uncontrolled recursion could allow an attacker to cause a panic due to stack exhaustion via deeply nested types or declarations. This issue has been resolved in MTA version 6.2.2.

For more details, see (CVE-2022-1962).

CVE-2023-26159: Improper handling of URLs by the url.parse() function

In versions of the **follow-redirects** package before 1.15.4, there is a vulnerability to Improper Input Validation. This flaw is caused by the improper handling of URLs by the **url.parse()** function. When new **URL()** throws an error, it can be manipulated to misinterpret the hostname. An attacker could exploit this weakness to redirect traffic to a malicious site, and could lead to information disclosure, phishing attacks, or other security breaches. This issue has been resolved in MTA version 6.2.2.

For more details, see (CVE-2023-26159).

CVE-2022-46751: Improper Restriction of XML External Entity Reference, XML Injection vulnerability in Apache Ivy

In version of Apache Ivy before 2.5.2, parsing XML files, either its configuration, Ivy files or Apache Maven POMs, it allows downloading external document type definitions and expand any entity references contained. This process can be used to exfiltrate data, access resources only the machine running Ivy has access to, or disturb the execution of Ivy in different ways. This issue has been resolved in MTA version 6.2.2.

For more details, see (CVE-2022-46751).

CVE-2023-2976: Java's default temporary directory for file creation in FileBackedOutputStream

Version of Google Guava versions 1.0 to 31.1 could allow a local authenticated attacker to obtain sensitive information. This is caused by a flaw with using Java's default temporary directory for file creation in **FileBackedOutputStream**. Using Java's default temporary directory for file creation in **FileBackedOutputStream** on Unix systems, could allow other users and apps on the machine with access to the default Java temporary directory to be able to access the files created by the class. This issue has been resolved in MTA version 6.2.2.

For more details, see (CVE-2023-2976).

CVE-2023-35116: Versions of jackson-databind before 2.15.2 could allow attackers to cause a denial of service or other unspecified impact (disputed)

Versions of **jackson-databind** before 2.15.2 could allow attackers to cause a denial of service or other unspecified impact. The vendor believes that this is not a valid vulnerability because the steps of constructing a cyclic data structure and trying to serialize it cannot be achieved by an external attacker. This issue has been resolved in MTA version 6.2.2.

For more details, see (CVE-2023-35116).

CVE-2023-1436: An infinite recursion is triggered in Jettison when constructing a JSONArray

An infinite recursion is triggered in Jettison when constructing a **JSONArray** from a Collection that contains a self-reference in one of its elements. This leads to a **StackOverflowError** exception being returned. This issue has been resolved in MTA version 6.2.2.

For more details, see (CVE-2023-1436).

For a complete list of all issues resolved in this release, see the list of Resolved Issues in Jira .

2.2. KNOWN ISSUES

Migration Toolkit for Applications (MTA) version 6.2.2 has the following issues.

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

Loop with Unreachable Exit Condition, **Infinite Loop**, vulnerability in Apache Commons Compress. This vulnerability affects Apache Commons Compress, versions 1.3 to 1.25.0, and can lead to a Denial of Service (DoS).

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

CVE-2023-6291: Keycloak redirect_uri validation bypass

An issue was found in the **redirect_uri** validation logic in Keycloak that allows for a bypass of otherwise explicitly allowed hosts. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to an access token being stolen, making it possible for the attacker to impersonate other users.

For more details, see (CVE-2023-6291).

CVE-2024-1300: Eclipse Vert.x memory leak when a TCP server is configured with TLS and SNI support

A vulnerability in the Eclipse Vert.x toolkit causes a memory leak in TCP servers configured with Transport Layer Security (TLS) and Server Name Indication (SNI) support. When processing an unknown SNI server name assigned the default certificate instead of a mapped certificate, the Secure Sockets Layer (SSL) context is mistakenly cached in the server name map, leading to memory exhaustion. This issue could allow attackers to send TLS client **hello** messages with fake server names, triggering a Java virtual machine (JVM) Out-of-Memory (OOM) error.

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

CVE-2023-45286

A race condition in **go-resty** can result in HTTP request body disclosure across requests. This condition can be triggered by calling **sync.Pool.Put** with the same ***bytes.Buffer** more than once, when request retries are enabled and a retry occurs. The call to **sync.Pool.Get** will then return a **bytes.Buffer** that has not had **bytes.Buffer.Reset** called on it. This dirty buffer will contain the HTTP request body from an unrelated request, and **go-resty** will append the current HTTP request body to it, sending two bodies in one request. The **sync.Pool** in question is defined at package level scope, so a completely unrelated server could receive the request body.

For more details, see (CVE-2023-45286).

CVE-2023-48631: Adobe's css-tools versions 4.3.1 and earlier are affected by an Improper Input Validation vulnerability

A Regular Expression Denial of Service (ReDoS) vulnerability was found in Adobe's **css-tools** when parsing CSS. This issue occurs due to improper input validation and may allow an attacker to use a carefully crafted input string to cause a denial of service, when attempting to parse CSS.

For more details, see (CVE-2023-48631).

CVE-2023-36479: Improper addition of quotation marks to user inputs in CgiServlet

Eclipse Jetty Canonical Repository is the canonical repository for the Jetty project. Users of the **CgiServlet** with a specific command structure may have the wrong command executed. If a user sends a request to an

org.eclipse.jetty.servlets.CGI Servlet for a binary with a space in its name, the servlet will escape the command by wrapping it in quotation marks. This wrapped command, plus an optional command prefix, will then be executed through a call to **Runtime.exec**. If the original binary name provided by the user contains a quotation mark followed by a space, the resulting command line will contain multiple tokens instead of one. This issue was patched in version 9.4.52, 10.0.16, 11.0.16 and 12.0.0-beta2.

For more details, see (CVE-2023-36479).

For a complete list of all known issues in this release, see the list of Known Issues in Jira .

CHAPTER 3. MTA 6.2.1

3.1. RESOLVED ISSUES

The following highlighted issues have been resolved in MTA version 6.2.1.

CVE-2023-44487 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. In previous releases of MTA, the HTTP/2 protocol allowed a denial of service (server resource consumption) because request cancellation could reset multiple streams quickly. The server had to set up and tear down the streams while not hitting any server-side limit for the maximum number of active streams per connection, which resulted in a denial of service due to server resource consumption.

The following issues have been listed under this issue:

- (MTA-1428)
- (MTA-1430)
- (MTA-1448)

To resolve this issue, upgrade to MTA 6.2.1 or later.

For more information, see CVE-2023-44487 (Rapid Reset Attack) .

CVE-2023-39325: Multiple HTTP/2 enabled web servers are vulnerable to a DDoS attack (Rapid Reset Attack in the Go language packages)

The HTTP/2 protocol is susceptible to a denial of service attack because request cancellation can reset multiple streams quickly. The server has to set up and tear down the streams while not hitting any server-side limit for the maximum number of active streams per connection. This results in a denial of service due to server resource consumption.

The following issues have been listed under this issue:

- MTA-1429
- MTA-1482
- MTA-1447

To resolve this issue, upgrade to MTA 6.2.1 or later.

For more information, see CVE-2023-39325 (Rapid Reset Attack in the Go language packages) .

CHAPTER 4. MTA 6.2.0

4.1. NEW FEATURES

This section describes the new features of the Migration Toolkit for Applications (MTA) 6.2.0.

Integration with JIRA

The integration of Migration Toolkit for Applications with Jira allows you to track and manage the whole migration process. To introduce changes to the applications in the portfolio, you can create issues in Jira and assign them to developers.

For more information, see Creating and configuring a Jira connection .

Migration Waves management

A migration wave is a small collection of workloads that deliver business value. MTA's *Migration Wave* groups applications to be migrated on a specified schedule.

In addition, a migration wave enables you to export a list of the wave's applications to the Jira issue management system. This automatically creates a separate Jira issue for each application of the migration wave for tracking.

For more information, see Creating migration waves and Creating Jira issues for a migration wave .

OpenShift Monitoring integration

MTA integrates with OpenShift Monitoring, which allows users to consume metrics from their MTA installation.

4.2. KNOWN ISSUES

MTA version 6.2.0 has the following issues.

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

A flaw has been found in handling multiplexed streams in the HTTP/2 protocol. The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can be reset multiple streams quickly. The server has to set up and tear down the streams while not hitting any server-side limit for the maximum number of active streams per connection, which resulted in a denial of service due to server resource consumption.

The following issues have been listed under this issue:

- (MTA-1428)
- (MTA-1430)
- (MTA-1448)

To resolve this issue, upgrade to MTA 6.2.1 or later.

For more details, see CVE-2023-44487 (Rapid Reset Attack)

CVE-2023-39325: Multiple HTTP/2 enabled web servers are vulnerable to a DDoS attack (Rapid Reset Attack in the Go language packages)

The HTTP/2 protocol is susceptible to a denial of service attack because request cancellation can reset multiple streams quickly. The server has to set up and tear down the streams while not hitting any server-side limit for the maximum number of active streams per connection. This results in a denial of service due to server resource consumption.

The following issues have been listed under this issue:

- MTA-1429
- MTA-1482
- MTA-1447

To resolve this issue, upgrade to MTA 6.2.1 or later.

For more information, see CVE-2023-39325 (Rapid Reset Attack in the Go language packages) .

Re-enabling Keycloak breaks MTA

Keycloak is enabled by default. If you disable and then re-enable Keycloak, you cannot perform any actions in the MTA web console after logging in again.

This error is caused as the **credential-mta-rhsso** secret is updated when **auth/Keycloak** is disabled and re-enabled.

The suggested workaround is to restore the old password in the **credential-mta-rhsso** secret, after re-enabling **auth**. MTA-1152

Analysis fails when fetching rules from a repository with a folder that contains spaces in its name

When fetching custom rules from a repository during an analysis, if the **Root path** field contains spaces, the **mta-cli** command is not properly composed and the analysis fails. MTA-458

Update notifications are disabled for Application, Job functions, and Business services

Update notifications are disabled for **Application**, **Job function** and **Business services**, as a result, no notifications are displayed. MTA-1024

Repository type field is not required

The **Repository type** field is not required when saving the configuring rules files from a repository in analysis. MTA-1047

False 'not connected' status for new Jira instance

When creating a new Jira instance, the connection status is initially shown as **Not connected** before it moves to **Connected**, and this delay could cause the user to think that the provided credentials are incorrect. MTA-1019

For a complete list of all known issues in this release, see the list of Known Issues in Jira .

4.3. RESOLVED ISSUES

The following highlighted issues have been resolved in MTA version 6.2.0.

Analysis wizard

The release of MTA 6.2.0 resolves the issue that Analysis wizard was stuck on the custom rules page on moving **Back** from the Repository tab. For more information on this issue, see MTA-464.

Tags & Reports tabs

The release of MTA 6.2.0 resolves the issue that an analysis was running for an application, and after clicking on that application to see the Tags and Reports, both the tabs keep loading until the analysis finished. For more information on this issue, see MTA-465.

For a complete list of all issues resolved in this release, see the list of Resolved Issues in Jira .