RHSA-2024:1353 - Security Advisory

Issued: 2024-03-18 Updated: 2024-03-18

Overview

Synopsis

Important: Red Hat Process Automation Manager 7.13.5 security update

Type/Severity

Security Advisory: Important

Topic

An update is now available for Red Hat Process Automation Manager.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which provides a detailed severity rating, is available for each vulnerability from the CVE links in the References section.

Description

Red Hat Process Automation Manager is an open source business process management suite that combines process management and decision service management and enables business and IT users to create, manage, validate, and deploy process applications and decision services.

This asynchronous security patch is an update to Red Hat Process Automation Manager 7.

Security Fixes:

- JSON-java: parser confusion leads to OOM (CVE-2023-5072)
- okio: GzipSource class improper exception handling (CVE-2023-3635)
- xstream: Denial of Service by injecting recursive collections or maps based on element's hash values raising a stack overflow (CVE-2022-41966)

- batik: Server-Side Request Forgery vulnerability (CVE-2022-44729)
- batik: Server-Side Request Forgery vulnerability (CVE-2022-44730)
- bouncycastle: potential blind LDAP injection attack using a self-signed certificate (CVE-2023-33201)
- xstream: Xstream to serialise XML data was vulnerable to Denial of Service attacks (CVE-2022-40151)
- RESTEasy: creation of insecure temp files (CVE-2023-0482)
- snakeyaml: Constructor Deserialization Remote Code Execution (CVE-2022-1471)

For more details about the security issues, including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE pages listed in the References section.

Solution

Before applying this update, make sure all previously released errata relevant to your system have been applied.

For details on how to apply this update, refer to:

https://access.redhat.com/articles/11258

Affected Products

- Red Hat JBoss Middleware Text-Only Advisories for MIDDLEWARE 1 x86_64

Fixes

- BZ - 2134292 - CVE-2022-40151 xstream: Xstream to serialise XML data was vulnerable to Denial of Service attacks
- BZ - 2150009 - CVE-2022-1471 SnakeYaml: Constructor Deserialization Remote Code Execution
- BZ - 2166004 - CVE-2023-0482 RESTEasy: creation of insecure temp files
- BZ - 2170431 - CVE-2022-41966 xstream: Denial of Service by injecting recursive collections or maps based on element's hash values raising a stack overflow
- BZ - 2215465 - CVE-2023-33201 bouncycastle: potential blind LDAP injection attack using a self-signed certificate
- BZ - 2229295 - CVE-2023-3635 okio: GzipSource class improper exception handling
- BZ - 2233889 - CVE-2022-44729 batik: Server-Side Request Forgery vulnerability
- BZ - 2233899 - CVE-2022-44730 batik: Server-Side Request Forgery vulnerability
- BZ - 2246417 - CVE-2023-5072 JSON-java: parser confusion leads to OOM

CVEs

- CVE-2022-1471
- CVE-2022-40151

- CVE-2022-41966
- CVE-2022-44729
- CVE-2022-44730
- CVE-2023-0482
- CVE-2023-3635
- CVE-2023-5072
- CVE-2023-6481
- CVE-2023-6717
- CVE-2023-33201

References

- https://access.redhat.com/security/updates/classification/#important

---

The Red Hat security contact is secalert@redhat.com. More contact details at https://access.redhat.com/security/team/contact/.