May 6, 2024

Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Red Hat published security advisories to address vulnerabilities in multiple products. Included were updates to address vulnerabilities in the Linux kernel for the following products:

- Red Hat Enterprise Linux – multiple versions and platforms
- Red Hat Enterprise Linux Server – multiple versions and platforms
- Red Hat Virtualization Host 4 for RHEL 8 x86_64 – multiple versions
- Red Hat CodeReady Linux Builder – multiple versions and platforms

Technical Details

Red Hat build of Apache Camel 4.4.0 for Spring Boot release and security update is now available.
The purpose of this text-only errata is to inform you about the security issues fixed.
Security Fix(es):

- xnio: StackOverflowException when the chain of notifier states becomes problematically big (CVE-2023-5685)
- tomcat: Leaking of unrelated request bodies in default error page (CVE-2024-21733)
- guava: insecure temporary directory creation (CVE-2023-2976)
- jackson-databind: denial of service via cylic dependencies (CVE-2023-35116)
- json-path: stack-based buffer overflow in Criteria.parse method (CVE-2023-51074)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-5685 CVE-2024-21733 CVE-2023-2976 CVE-2023-35116 CVE-2023-51074 CVE-2024-30156 CVE-2023-45288 CVE-2023-6546 CVE-2024-1086 CVE-2023-50387 CVE-2023-50868 CVE-2024-1753 CVE-2024-28180
- Red Hat Security Advisories