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 OpenShift Container Platform release 4.13.5 is now available. This release includes a security update for Red Hat OpenShift Container Platform 4.13.

Affected Products

- Red Hat OpenShift Container Platform 4.13 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.13 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.13 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.13 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.13 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.13 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.13 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.13 for RHEL 8 aarch64

Technical Details

Security Fixes:

- golang: net/http: excessive memory growth in a Go server accepting HTTP/2 requests (CVE-2022-41717)
- net/http, golang.org/x/net/http2: avoid quadratic complexity in HPACK decoding (CVE-2022-41723)
- distribution/distribution: DoS from malicious API request (CVE-2023-2253)

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

- https://access.redhat.com/security/updates/classification/#moderate
- https://docs.openshift.com/container-platform/4.13/release_notes/ocp-4-12-release-notes.html