July 4, 2024

Overall Rating: High

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of multiple Red Hat Security Advisories impacting numerous Red Hat products.

Technical Details

Please consult the Red Hat Security Advisories linked below for detailed information on the vulnerabilities and products impacted.

Advisory Link	Synopsis	Severity
RHSA-2024:4197 - Security Advisory	httpd:2.4 module is now available for Red Hat Enterprise Linux 8.	**MEDIUM**
RHSA-2024:4179 - Security Advisory	pki-core is now available for Red Hat Enterprise Linux 8.8 Extended Update Support.	**HIGH**
RHSA-2024:3617 - Security Advisory	Kube Descheduler Operator for Red Hat OpenShift 5.0.1 for RHEL 9	**MEDIUM**
RHSA-2024:3637 - Security Advisory	Secondary Scheduler Operator for Red Hat OpenShift 1.3.0 for RHEL 9	**MEDIUM**
RHSA-2024:1616 - Security Advisory	Run Once Duration Override Operator for Red Hat OpenShift 1.1.1 for RHEL 9	**HIGH**
RHSA-2024:4166 - Security Advisory	update for python3 is now available for Red Hat Enterprise Linux 8.2 Advanced Update Support.	**HIGH**
RHSA-2024:4165 - Security Advisory	update for pki-core is now available for Red Hat Enterprise Linux 9.	**HIGH**
RHSA-2024:4164 - Security Advisory	update for pki-core is now available for Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support, Red Hat Enterprise Linux 8.4 Update Services for SAP Solutions, and Red Hat Enterprise Linux 8.4 Telecommunications Update Service.	**HIGH**
RHSA-2024:0043 - Security Advisory	MicroShift release 4.16.0 is now available with updates to packages and images that include a security update.	**MEDIUM**
RHSA-2024:4163 - Security Advisory	Errata Advisory for Red Hat OpenShift GitOps v1.12.4 security update	**HIGH**
RHSA-2024:0045 - Security Advisory	OpenShift Container Platform 4.16.0 security update	**HIGH**
RHSA-2024:0041 - Security Advisory	OpenShift Container Platform 4.16.0 bug fix and security update	**HIGH**
RHSA-2024:0040 - Security Advisory	OpenShift Container Platform 4.16.0 security and extras update	**HIGH**

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have atVulnerabilityandRiskManagement@gov.bc.ca.

References

- CVE-2023-38709, CVE-2023-4727, CVE-2024-24783, CVE-2024-24784, CVE-2024-24785, CVE-2024-24786, CVE-2023-45288, CVE-2023-45290, CVE-2023-7104, CVE-2023-6597, CVE-2021-25220, CVE-2022-2795, CVE-2022-3094, CVE-2023-4408, CVE-2023-6597, CVE-2023-45288, CVE-2023-45289, CVE-2023-45290, CVE-2023-50387, CVE-2023-50868, CVE-2023-52425, CVE-2024-0450, CVE-2024-2961, CVE-2024-24783, CVE-2024-24786, CVE-2024-25062, CVE-2024-25620, CVE-2024-26147, CVE-2024-28834, CVE-2024-33599, CVE-2024-33600, CVE-2024-33601, CVE-2024-33602, CVE-2023-29483, CVE-2024-3727, CVE-2024-28176, CVE-2019-25210, CVE-2023-45142, CVE-2023-48795, CVE-2024-0874, CVE-2024-22189, CVE-2024-2398, CVE-2024-28110, CVE-2024-28180, CVE-2024-28757, CVE-2024-28849, CVE-2024-29180, CVE-2024-28182
- Red Hat Security Advisory
- VRM Vulnerability Reports