RHSA-2024:1566 - Security Advisory

Issued: 2024-04-03 Updated: 2024-04-03

Synopsis

Important: Red Hat build of MicroShift 4.14.19 security update

Type/Severity

Security Advisory: Important

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

View affected systems

Topic

Red Hat build of MicroShift release 4.14.19 is now available with updates to packages and images that fix several bugs and add enhancements.

This release includes a security update for Red Hat build of MicroShift 4.14.

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

Description

Red Hat build of MicroShift is Red Hat's light-weight Kubernetes orchestration solution designed for edge device deployments and is built from the edge capabilities of Red Hat OpenShift. MicroShift is an application that is deployed on top of Red Hat Enterprise Linux devices at the edge, providing an efficient way to operate single-node clusters in these low-resource environments.

This advisory contains the RPM packages for Red Hat build of MicroShift 4.14.z. Read the following advisory for the container images for this release:

https://access.redhat.com/errata/RHBA-2024:1564

Security Fix(es):

- golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads (CVE-2024-1394)

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.

All of the bug fixes may not be documented in this advisory. Read the following release notes for details about these changes:

https://access.redhat.com/documentation/en-us/red_hat_build_of_microshift/4.14/html/release_notes/index

All Red Hat build of MicroShift 4.14 users are advised to use these updated packages and images when they are available in the RPM repository.

Solution

For MicroShift 4.14, read the following documentation, which will be updated shortly for this release, for important instructions on how to install the latest RPMs and fully apply this asynchronous errata update:

https://access.redhat.com/documentation/en-us/red_hat_build_of_microshift/4.14/html/release_notes/index

Affected Products

- Red Hat OpenShift Container Platform 4.14 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform for ARM 64 4.14 for RHEL 9 aarch64

Fixes

- BZ - 2262921 - CVE-2024-1394 golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads

CVEs

- CVE-2024-1394

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/.

Loading

About Red Hat
Jobs
Events
Locations
Contact Red Hat
Red Hat Blog
Inclusion at Red Hat
Cool Stuff Store
Red Hat Summit

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility
Cookie preferences