Red Hat F

RHSA
Advis

-05-05

Overview

Updated Ir

Synop

Importa

Type/Severity

Security Advisory: Important

Topic

Updated RHEL-8 based Middleware Containers container images are now available

Description

The RHEL-8 based Middleware Containers container images have been updated to address the following security advisory:
RHSA-2026:11077
RHSA-2026:7667
RHSA-2026:8534
RHSA-2026:9745
(see References)

Security Fixes:

- rsync: Rsync: Out of bounds array access via negative index (CVE-2025-10158)

- gnutls: Stack-based Buffer Overflow in gnutls_pkcs11_token_init() Function (CVE-2025-9820)
- gnutls: GnuTLS: Denial of Service via excessive resource consumption during certificate verification (CVE-2025-14831)
- openssh: OpenSSH GSSAPI: Information disclosure or denial of service due to uninitialized variables (CVE-2026-3497)
- nghttp2: nghttp2: Denial of Service via malformed HTTP/2 frames after session termination (CVE-2026-27135)
- libarchive: libarchive: Information disclosure via heap out-of-bounds read in RAR archive processing (CVE-2026-4424)
- python: Python: Command-line option injection in webbrowser.open() via crafted URLs (CVE-2026-4519)
- libarchive: libarchive: Arbitrary code execution via integer overflow in ISO9660 image processing (CVE-2026-5121)
- python: Python: Arbitrary code execution or information disclosure via use-after-free in decompression modules (CVE-2026-6100)
- python: cpython: Python: Arbitrary code execution via command injection in webbrowser.open() API (CVE-2026-4786)

Users of RHEL-8 based Middleware Containers container images are advised to upgrade to these updated images, which contain backported patches to correct these security issues, fix these bugs and add these enhancements. Users of these images are also encouraged to rebuild all container images that depend on these images.

You can find images updated by this advisory in Red Hat Container Catalog (see References).

Solution

The RHEL-8 based Middleware Containers container images provided by this update can be downloaded from the Red Hat Container Registry at registry.access.redhat.com. Installation instructions for your platform are available at Red Hat Container Catalog (see References).

Dockerfiles and scripts should be amended either to refer to this new image specifically, or to the latest image generally.

Affected Products

- Red Hat OpenShift Container Platform 4.12 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform 4.11 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform 4.10 for RHEL 8 x86_64

Fixes

- BZ - 2392528 - CVE-2025-9820 gnutls: Stack-based Buffer Overflow in gnutls_pkcs11_token_init() Function

- BZ - 2415637 - CVE-2025-10158 rsync: Rsync: Out of bounds array access via negative index
- BZ - 2423177 - CVE-2025-14831 gnutls: GnuTLS: Denial of Service via excessive resource consumption during certificate verification
- BZ - 2447085 - CVE-2026-3497 openssh: OpenSSH GSSAPI: Information disclosure or denial of service due to uninitialized variables
- BZ - 2448754 - CVE-2026-27135 nghttp2: nghttp2: Denial of Service via malformed HTTP/2 frames after session termination
- BZ - 2449006 - CVE-2026-4424 libarchive: libarchive: Information disclosure via heap out-of-bounds read in RAR archive processing
- BZ - 2449649 - CVE-2026-4519 python: Python: Command-line option injection in webbrowser.open() via crafted URLs
- BZ - 2452945 - CVE-2026-5121 libarchive: libarchive: Arbitrary code execution via integer overflow in ISO9660 image processing
- BZ - 2457932 - CVE-2026-6100 python: Python: Arbitrary code execution or information disclosure via use-after-free in decompression modules
- BZ - 2458049 - CVE-2026-4786 python: cpython: Python: Arbitrary code execution via command injection in webbrowser.open() API

CVEs

- CVE-2025-9820
- CVE-2025-10158
- CVE-2025-14831
- CVE-2026-3497
- CVE-2026-4424
- CVE-2026-4519
- CVE-2026-4786
- CVE-2026-5121
- CVE-2026-6100
- CVE-2026-27135

References

- https://access.redhat.com/security/updates/classification/#important
- https://access.redhat.com/errata/RHSA-2026:11077
- https://access.redhat.com/errata/RHSA-2026:7667
- https://access.redhat.com/errata/RHSA-2026:8534
- https://access.redhat.com/errata/RHSA-2026:9745
- https://errata.engineering.redhat.com/advisory/165062
- https://access.redhat.com/containers

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