



Red Hat F

# RHSA



5-07-17

Overview

Updated In

## 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-2025:10698 (see References)

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](https://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 - 2370010](#)  - CVE-2025-4435 cpython: Tarfile extracts filtered members when errorlevel=0
- [BZ - 2370013](#)  - CVE-2024-12718 cpython: python: Bypass extraction filter to modify file metadata outside extraction directory
- [BZ - 2370014](#)  - CVE-2025-4330 cpython: python: Extraction filter bypass for linking outside extraction directory
- [BZ - 2370016](#)  - CVE-2025-4517 python: cpython: Arbitrary writes via tarfile realpath overflow
- [BZ - 2372373](#)  - CVE-2025-49794 libxml: Heap use after free (UAF) leads to Denial of service (DoS)
- [BZ - 2372385](#)  - CVE-2025-49796 libxml: Type confusion leads to Denial of service (DoS)
- [BZ - 2372406](#)  - CVE-2025-6021 libxml2: Integer Overflow in xmlBuildQName() Leads to Stack Buffer Overflow in libxml2
- [BZ - 2372426](#)  - CVE-2025-4138 cpython: python: Bypassing extraction filter to create symlinks to arbitrary targets outside extraction directory
- [BZ - 2372512](#)  - CVE-2025-6020 linux-pam: Linux-pam directory Traversal

## CVEs

- [CVE-2024-12718](#) 
- [CVE-2025-4138](#) 
- [CVE-2025-4330](#) 
- [CVE-2025-4435](#) 
- [CVE-2025-4517](#) 
- [CVE-2025-6020](#) 
- [CVE-2025-6021](#) 

- [CVE-2025-49794](#) ↗
- [CVE-2025-49796](#) ↗

## References

- <https://access.redhat.com/security/updates/classification/#important> ↗
- <https://access.redhat.com/errata/RHSA-2025:10698> ↗
- <https://access.redhat.com/containers> ↗

The Red Hat security contact is [secalert@redhat.com](mailto:secalert@redhat.com). More contact details at <https://access.redhat.com/security/team/contact/>.



---

Quick Links 


---

Help 


---

Site Info 

---

Related Sites 

---

 All systems operational



About Red Hat

Jobs

Events

Locations

[Contact Red Hat](#)

[Red Hat Blog](#)

[Inclusion at Red Hat](#)

[Cool Stuff Store](#)

[Red Hat Summit](#)

---

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie Preferences and Do Not Sell or Share My Personal Information](#)