[RHSA-2022:6024-01] Moderate: New container image for R...

Article URL
www.securityhome.eu/mailings/mailing.php?mid=21211

Author
SecurityHome.eu

Published: 10 August 2022

==========
Red Hat Security Advisory

Synopsis: Moderate: New container image for Red Hat Ceph Storage 5.2 Security update
Advisory ID: RHSA-2022:6024-01
Product: Red Hat Ceph Storage
Advisory URL: https://access.redhat.com/errata/RHSA-2022:6024
Issue date: 2022-08-09
CVE Names: CVE-2021-40528 CVE-2021-43813 CVE-2022-0670
CVE-2022-1292 CVE-2022-1586 CVE-2022-1785
CVE-2022-1897 CVE-2022-1927 CVE-2022-2068
CVE-2022-2097 CVE-2022-21673 CVE-2022-22576
CVE-2022-25313 CVE-2022-25314 CVE-2022-27774
CVE-2022-27776 CVE-2022-27782 CVE-2022-29824
==========
1. Summary:

A new container image for Red Hat Ceph Storage 5.2 is now available in the
Red Hat Ecosystem Catalog.

Red Hat Product Security has rated this update as having a security impact
of Moderate. 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.

2. Description:

Red Hat Ceph Storage is a scalable, open, software-defined storage platform
that combines the most stable version of the Ceph storage system with a
Ceph management platform, deployment utilities, and support services.

This new container image is based on Red Hat Ceph Storage 5.2 and Red Hat
Enterprise Linux 8.6 and Red Hat Enterprise Linux 9.

Space precludes documenting all of these changes in this advisory. Users are directed to the Red Hat Ceph Storage Release Notes for information on the most significant of these changes:

https://access.redhat.com/documentation/en-us/red_hat_ceph_storage/5.2/html-single/release_notes/index

All users of Red Hat Ceph Storage are advised to pull these new images from the Red Hat Ecosystem catalog, which provides numerous enhancements and bug fixes.

Security Fix(es):

* grafana: Forward OAuth Identity Token can allow users to access some data sources (CVE-2022-21673)

* grafana: directory traversal vulnerability (CVE-2021-43813)

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.

3. Solution:

Before applying this update, make sure all previously released errata relevant to your system have been applied.

For details on how to apply this update, refer to:

https://access.redhat.com/articles/2789521

For supported configurations, refer to:

https://access.redhat.com/articles/1548993

4. Bugs fixed (https://bugzilla.redhat.com/):

2031228 - CVE-2021-43813 grafana: directory traversal vulnerability
2044628 - CVE-2022-21673 grafana: Forward OAuth Identity Token can allow users to access some data sources
2115198 - build ceph containers for RHCS 5.2 release

5. References:

https://access.redhat.com/security/cve/CVE-2021-40528
https://access.redhat.com/security/cve/CVE-2021-43813
https://access.redhat.com/security/cve/CVE-2022-0670
https://access.redhat.com/security/cve/CVE-2022-1292

https://access.redhat.com/security/cve/CVE-2022-1586
https://access.redhat.com/security/cve/CVE-2022-1785
https://access.redhat.com/security/cve/CVE-2022-1897
https://access.redhat.com/security/cve/CVE-2022-1927
https://access.redhat.com/security/cve/CVE-2022-2068
https://access.redhat.com/security/cve/CVE-2022-2097
https://access.redhat.com/security/cve/CVE-2022-21673
https://access.redhat.com/security/cve/CVE-2022-22576
https://access.redhat.com/security/cve/CVE-2022-25313
https://access.redhat.com/security/cve/CVE-2022-25314
https://access.redhat.com/security/cve/CVE-2022-27774
https://access.redhat.com/security/cve/CVE-2022-27776
https://access.redhat.com/security/cve/CVE-2022-27782
https://access.redhat.com/security/cve/CVE-2022-29824
https://access.redhat.com/security/updates/classification/#moderate

6. Contact:

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