RHSA-2025:8479 - Security Advisory

Issued: 2025-06-04 Updated: 2025-06-04

Synopsis

Important: RHODF-4.16-RHEL-9 security update

Type/Severity

Security Advisory: Important

Topic

Updated images are now available for RHODF-4.16-RHEL-9.

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

OpenShift Data Foundation is software-defined storage integrated with and optimized for the Red Hat OpenShift Data Foundation. Red Hat OpenShift DataFoundation is a highly scalable, production-grade persistent storage for stateful applications running in the Red Hat OpenShift Container Platform. In addition to persistent storage, Red Hat OpenShift Data Foundation provisions a multi-cloud data management service with an S3 compatible API.

Security Fix(es):

- express: cause malformed URLs to be evaluated (CVE-2024-29041)
- nodejs-async: Regular expression denial of service while parsing function in autoinject (CVE-2024-39249)
- body-parser: Denial of Service Vulnerability in body-parser (CVE-2024-45590)
- npm-serialize-javascript: Cross-site Scripting (XSS) in serialize-javascript (CVE-2024-11831)
- http-proxy-middleware: Denial of Service (CVE-2024-21536)
- golang.org/x/net/html: Non-linear parsing of case-insensitive content in golang.org/x/net/html (CVE-2024-45338)
- golang-jwt/jwt: jwt-go allows excessive memory allocation during header parsing (CVE-2025-30204)

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.

Solution

For details on how to apply this update, which includes the changes described in this advisory, refer to:

https://access.redhat.com/articles/11258

Affected Products

- Red Hat OpenShift Data Foundation 4 for RHEL 9 x86_64
- Red Hat OpenShift Data Foundation for IBM Power, little endian 4 for RHEL 9 ppc64le
- Red Hat OpenShift Data Foundation for IBM Z and LinuxONE 4 for RHEL 9 s390x
- Red Hat OpenShift Data Foundation for RHEL 9 ARM 4 aarch64

Fixes

- BZ - 2290901 - CVE-2024-29041 express: cause malformed URLs to be evaluated
- BZ - 2295035 - CVE-2024-39249 nodejs-async: Regular expression denial of service while parsing function in autoinject
- BZ - 2311171 - CVE-2024-45590 body-parser: Denial of Service Vulnerability in body-parser
- BZ - 2312579 - CVE-2024-11831 npm-serialize-javascript: Cross-site Scripting (XSS) in serialize-javascript
- BZ - 2319884 - CVE-2024-21536 http-proxy-middleware: Denial of Service
- BZ - 2333122 - CVE-2024-45338 golang.org/x/net/html: Non-linear parsing of case-insensitive content in golang.org/x/net/html
- BZ - 2354195 - CVE-2025-30204 golang-jwt/jwt: jwt-go allows excessive memory allocation during header parsing
- DFBUGS-1702 - [Backport to 4.16.z] rook-ceph-osd-prepare-ocs-deviceset pods produce duplicate metrics

- DFBUGS-714 - [2316908] [ODF 4.16 backport]cluster-cleanup-job pod not cleaning /var/lib/rook
- DFBUGS-2603 - [Critical] Upgrade ceph version to RHCEPH-7.1z4 at ODF-4.16.10

CVEs

- CVE-2023-23934
- CVE-2023-25577
- CVE-2023-46446
- CVE-2023-48795
- CVE-2024-8176
- CVE-2024-11831
- CVE-2024-21536
- CVE-2024-24790
- CVE-2024-29041
- CVE-2024-34069
- CVE-2024-39249
- CVE-2024-42353
- CVE-2024-45338
- CVE-2024-45590
- CVE-2024-47191
- CVE-2024-48916
- CVE-2025-0395
- CVE-2025-27516
- CVE-2025-30204

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/.

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

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility
Cookie Preferences and Opt-Out Rights