



RHSA-2025:4511 - Security Advisory

 Issued: 2025-05-06 Updated: 2025-05-06[Overview](#)[Updated Images](#)

Synopsis

Important: RHODF-4.18-RHEL-9 security update

Type/Severity

Security Advisory: Important

Topic

Updated images are now available for RHODF-4.18-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 Data Foundation 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)

- `npm-serialize-javascript`: Cross-site Scripting (XSS) in `serialize-javascript` (CVE-2024-11831)
- `http-proxy-middleware`: Denial of Service (CVE-2024-21536)
- `go-jose`: Go JOSE's Parsing Vulnerable to Denial of Service (CVE-2025-27144)
- `golang.org/x/oauth2/jws`: Unexpected memory consumption during token parsing in `golang.org/x/oauth2/jws` (CVE-2025-22868)
- `golang.org/x/crypto/ssh`: Denial of Service in the Key Exchange of `golang.org/x/crypto/ssh` (CVE-2025-22869)
- `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 - 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 - 2347423](#) - CVE-2025-27144 `go-jose`: Go JOSE's Parsing Vulnerable to Denial of Service
- [BZ - 2348366](#) - CVE-2025-22868 `golang.org/x/oauth2/jws`: Unexpected memory consumption during token parsing in `golang.org/x/oauth2/jws`
- [BZ - 2348367](#) - CVE-2025-22869 `golang.org/x/crypto/ssh`: Denial of Service in the Key Exchange of `golang.org/x/crypto/ssh`
- [BZ - 2354195](#) - CVE-2025-30204 `golang-jwt/jwt`: `jwt-go` allows excessive memory allocation during header parsing
- [DFBUGS-1798](#) - [4.18 clone][2319814] [RDR] Volsync Job Name exceeds 63 characters when application PVC exceeds 42 characters

- [DFBUGS-269](#) - [2312445] [ODF on ROSA HCP] must-gather fail to collect noobaa_diagnostics.tar.gz

CVEs

- [CVE-2024-8176](#)
- [CVE-2024-11831](#)
- [CVE-2024-21536](#)
- [CVE-2024-29041](#)
- [CVE-2025-0395](#)
- [CVE-2025-22868](#)
- [CVE-2025-22869](#)
- [CVE-2025-27144](#)
- [CVE-2025-27363](#)
- [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 ▼

 Partial system outage



[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](#)