



Red Hat Product Errata RHSA-2026:9742 - Security Advisory

RHSA-2026:9742 - Security Advisory

Issued: 2026-04-22 Updated: 2026-04-22

[Overview](#)[Updated Images](#)

Synopsis

Red Hat Developer Hub 1.8.6 release.

Type/Severity

Security Advisory: Critical

Topic

Red Hat Developer Hub 1.8.6 has been released.



Description

Red Hat Developer Hub (RHDH) is Red Hat's enterprise-grade, self-managed, customizable developer portal based on Backstage.io. RHDH is supported on OpenShift and other major Kubernetes clusters (AKS, EKS, GKE). The core features of RHDH include a single pane of glass, a centralized software catalog, self-service via golden path templates, and Tech Docs. RHDH is extensible by plugins.



























Solution

For more about Red Hat Developer Hub, see [References links](#)






Fixes

























- [RHDHBUGS-2288](#)  - Error while loading PagerDuty backend plugin
- [RHDHBUGS-2947](#)  - [Docs] - Update the Compatibility guide for Orchestrator and the 1.1. Red Hat supported plugins

CVEs

- [CVE-2025-62718](#) 
- [CVE-2025-69534](#) 
- [CVE-2025-69873](#) 
- [CVE-2026-1525](#) 
- [CVE-2026-1526](#) 
- [CVE-2026-1528](#) 
- [CVE-2026-2229](#) 
- [CVE-2026-25679](#) 
- [CVE-2026-26996](#) 
- [CVE-2026-27601](#) 
- [CVE-2026-27904](#) 
- [CVE-2026-29063](#) 
- [CVE-2026-29074](#) 
- [CVE-2026-29186](#) 
- [CVE-2026-3118](#) 
- [CVE-2026-32141](#) 
- [CVE-2026-33036](#) 
- [CVE-2026-33228](#) 
- [CVE-2026-33891](#) 
- [CVE-2026-33894](#) 
- [CVE-2026-33895](#) 
- [CVE-2026-33896](#) 
- [CVE-2026-39983](#) 
- [CVE-2026-40175](#) 
- [CVE-2026-4800](#) 
- [CVE-2026-4926](#) 

References

- <https://access.redhat.com/security/updates/classification/> 
- <https://catalog.redhat.com/search?gs&searchType=containers&q=rhdh> 
- <https://developers.redhat.com/rhdh/overview> 
- https://docs.redhat.com/en/documentation/red_hat_developer_hub 
- <https://issues.redhat.com/browse/RHDHBUGS-2288> 

- <https://issues.redhat.com/browse/RHDHBUGS-2947> 
- <https://issues.redhat.com/browse/RHDHBUGS-2972> 
- <https://issues.redhat.com/browse/RHIDP-12327> 
- <https://issues.redhat.com/browse/RHIDP-12388> 
- <https://issues.redhat.com/browse/RHIDP-12419> 
- <https://issues.redhat.com/browse/RHIDP-12511> 
- <https://issues.redhat.com/browse/RHIDP-12568> 
- <https://issues.redhat.com/browse/RHIDP-12647> 
- <https://issues.redhat.com/browse/RHIDP-12650> 
- <https://issues.redhat.com/browse/RHIDP-12655> 
- <https://issues.redhat.com/browse/RHIDP-12666> 
- <https://issues.redhat.com/browse/RHIDP-12686> 
- <https://issues.redhat.com/browse/RHIDP-12784> 
- <https://issues.redhat.com/browse/RHIDP-12880> 
- <https://issues.redhat.com/browse/RHIDP-12887> 
- <https://issues.redhat.com/browse/RHIDP-12921> 
- <https://issues.redhat.com/browse/RHIDP-12930> 
- <https://issues.redhat.com/browse/RHIDP-12996> 
- <https://issues.redhat.com/browse/RHIDP-13105> 
- <https://issues.redhat.com/browse/RHIDP-13107> 
- <https://issues.redhat.com/browse/RHIDP-13130> 
- <https://issues.redhat.com/browse/RHIDP-13180> 
- <https://issues.redhat.com/browse/RHIDP-13182> 
- <https://issues.redhat.com/browse/RHIDP-13185> 

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](#)

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie preferences](#)