



Red Hat Product Errata RHBA-2019:0327 - Bug Fix Advisory

RHBA-2019:0327 - Bug Fix Advisory

Issued: 2019-02-20

Updated: 2019-02-20

[Overview](#)

Synopsis

OpenShift Container Platform 3.11 images update

Type/Severity

Bug Fix Advisory

Topic

Red Hat OpenShift Container Platform release 3.11.82 is now available with updates to packages and images that fix several bugs.

Description

Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments.

This advisory contains the images for Red Hat OpenShift Container Platform 3.11.82. See the following advisory for the RPM packages for this release:

<https://access.redhat.com/errata/RHBA-2019:0326>

This update contains the following images:

openshift3/apb-base:v3.11.82-6
openshift3/apb-tools:v3.11.82-3
openshift3/automation-broker-apb:v3.11.82-6
openshift3/csi-attacher:v3.11.82-3
openshift3/csi-driver-registrar:v3.11.82-3

openshift3/csi-livenessprobe:v3.11.82-3
openshift3/csi-provisioner:v3.11.82-3
openshift3/grafana:v3.11.82-3
openshift3/jenkins-2-rhel7:v3.11.82-4
openshift3/jenkins-agent-maven-35-rhel7:v3.11.82-3
openshift3/jenkins-agent-nodejs-8-rhel7:v3.11.82-3
openshift3/jenkins-slave-base-rhel7:v3.11.82-4
openshift3/jenkins-slave-maven-rhel7:v3.11.82-4
openshift3/jenkins-slave-nodejs-rhel7:v3.11.82-4
openshift3/local-storage-provisioner:v3.11.82-3
openshift3/logging-fluentd:v3.11.82-3
openshift3/manila-provisioner:v3.11.82-3
openshift3/mariadb-apb:v3.11.82-6
openshift3/mediawiki-apb:v3.11.82-6
openshift3/mediawiki:v3.11.82-3
openshift3/metrics-cassandra:v3.11.82-3
openshift3/metrics-hawkular-metrics:v3.11.82-3
openshift3/metrics-hawkular-openshift-agent:v3.11.82-3
openshift3/metrics-heapster:v3.11.82-3
openshift3/metrics-schema-installer:v3.11.82-3
openshift3/mysql-apb:v3.11.82-6
openshift3/node:v3.11.82-3
openshift3/oauth-proxy:v3.11.82-3
openshift3/ose-ansible-service-broker:v3.11.82-3
openshift3/ose-ansible:v3.11.82-5
openshift3/ose-cli:v3.11.82-3
openshift3/ose-cluster-autoscaler:v3.11.82-3
openshift3/ose-cluster-capacity:v3.11.82-3
openshift3/ose-cluster-monitoring-operator:v3.11.82-4
openshift3/ose-configmap-reloader:v3.11.82-3
openshift3/ose-console:v3.11.82-3
openshift3/ose-deployer:v3.11.82-3
openshift3/ose-descheduler:v3.11.82-3
openshift3/ose-docker-builder:v3.11.82-3
openshift3/ose-docker-registry:v3.11.82-3
openshift3/ose-efs-provisioner:v3.11.82-3
openshift3/ose-egress-dns-proxy:v3.11.82-3
openshift3/ose-egress-http-proxy:v3.11.82-3
openshift3/ose-egress-router:v3.11.82-3
openshift3/ose-haproxy-router:v3.11.82-3


openshift3/ose-hyperkube:v3.11.82-3
openshift3/ose-hypershift:v3.11.82-3
openshift3/ose-keepalived-ipfailover:v3.11.82-3
openshift3/ose-kube-rbac-proxy:v3.11.82-3
openshift3/ose-kube-state-metrics:v3.11.82-3
openshift3/ose-logging-curator5:v3.11.82-5
openshift3/ose-logging-elasticsearch5:v3.11.82-6
openshift3/ose-logging-eventrouter:v3.11.82-3
openshift3/ose-logging-kibana5:v3.11.82-3
openshift3/ose-metrics-server:v3.11.82-3
openshift3/ose-node-problem-detector:v3.11.82-3
openshift3/ose-operator-lifecycle-manager:v3.11.82-3
openshift3/ose-ovn-kubernetes:v3.11.82-3
openshift3/ose-pod:v3.11.82-3
openshift3/ose-prometheus-config-reloader:v3.11.82-3
openshift3/ose-prometheus-operator:v3.11.82-3
openshift3/ose-recycler:v3.11.82-3
openshift3/ose-service-catalog:v3.11.82-3
openshift3/ose-template-service-broker:v3.11.82-3
openshift3/ose-tests:v3.11.82-3
openshift3/ose-web-console:v3.11.82-3
openshift3/ose:v3.11.82-3
openshift3/postgresql-apb:v3.11.82-6
openshift3/prometheus-alertmanager:v3.11.82-3
openshift3/prometheus-node-exporter:v3.11.82-3
openshift3/prometheus:v3.11.82-3
openshift3/registry-console:v3.11.82-3
openshift3/snapshot-controller:v3.11.82-3
openshift3/snapshot-provisioner:v3.11.82-3


All OpenShift Container Platform 3.11 users are advised to upgrade to these updated images.

Solution

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

See the following documentation, which will be updated shortly for release 3.11.82, for important instructions on how to upgrade your cluster and fully apply this asynchronous errata update:

https://docs.openshift.com/container-platform/3.11/release_notes/ocp_3_11_release_notes.html 

This update is available via the Red Hat Network. Details on how to use the Red Hat Network to apply this update are available at <https://access.redhat.com/articles/11258>. 































Affected Products

- Red Hat OpenShift Container Platform 3.11 x86_64

Fixes

- [BZ - 1676668](#)  - Placeholder for OCP 3.11 image refresh

CVEs

- [CVE-2017-16997](#) 
- [CVE-2017-18267](#) 
- [CVE-2018-1060](#) 
- [CVE-2018-1061](#) 
- [CVE-2018-1113](#) 
- [CVE-2018-5729](#) 
- [CVE-2018-5730](#) 
- [CVE-2018-5742](#) 
- [CVE-2018-6485](#) 
- [CVE-2018-7208](#) 
- [CVE-2018-7568](#) 
- [CVE-2018-7569](#) 
- [CVE-2018-7642](#) 
- [CVE-2018-7643](#) 
- [CVE-2018-8945](#) 
- [CVE-2018-10372](#) 
- [CVE-2018-10373](#) 
- [CVE-2018-10534](#) 
- [CVE-2018-10535](#) 
- [CVE-2018-10733](#) 
- [CVE-2018-10767](#) 
- [CVE-2018-10768](#) 
- [CVE-2018-11236](#) 
- [CVE-2018-11237](#) 
- [CVE-2018-12910](#) 
- [CVE-2018-13033](#) 
- [CVE-2018-13988](#) 
- [CVE-2018-15688](#) 
- [CVE-2018-16540](#) 
- [CVE-2018-16864](#) 

- [CVE-2018-16865](#)
- [CVE-2018-18311](#)
- [CVE-2018-18397](#)
- [CVE-2018-18559](#)
- [CVE-2018-19475](#)
- [CVE-2018-19476](#)
- [CVE-2018-19477](#)
- [CVE-2018-20102](#)
- [CVE-2018-20103](#)
- [CVE-2018-20615](#)
- [CVE-2018-1000007](#)
- [CVE-2018-1000120](#)
- [CVE-2018-1000121](#)
- [CVE-2018-1000122](#)
- [CVE-2018-1000301](#)
- [CVE-2018-1000865](#)
- [CVE-2018-1000866](#)
- [CVE-2019-3815](#)
- [CVE-2019-3818](#)
- [CVE-2019-3826](#)
- [CVE-2019-6116](#)
- [CVE-2019-1003000](#)
- [CVE-2019-1003001](#)
- [CVE-2019-1003002](#)
- [CVE-2019-1003003](#)
- [CVE-2019-1003004](#)
- [CVE-2019-1003010](#)
- [CVE-2019-1003011](#)
- [CVE-2019-1003012](#)
- [CVE-2019-1003013](#)
- [CVE-2019-1003014](#)

References

(none)

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