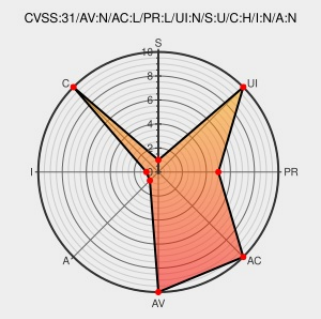
CVE-2019-10213

Published on: 11/25/2019 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:33:00 PM UTC

CVE-2019-10213

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Enterprise Linux from Redhat contain the following vulnerability:

OpenShift Container Platform, versions 4.1 and 4.2, does not sanitize secret data written to pod logs when the log level in a given operator is set to Debug or higher. A low privileged user could read pod logs to discover secret material if the log level has already been modified in an operator by a privileged user.

CVE-2019-10213 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Red Hat** - **openshift** version **= versions Red Hat OpenShift 4.1 and Red Hat OpenShift 4.2**

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
1734615 – (CVE-2019-10213) CVE-2019-10213 openshift: Secret data written	Issue Tracking	CONFIRM

to pod logs when operator set at Debug level or higher	Patch Vendor Advisory bugzilla.redhat.com text/html	bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10213
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2019:4088
1734615 – (CVE-2019-10213) CVE-2019-10213 openshift: Secret data written to pod logs when operator set at Debug level or higher	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1734615
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2019:4082
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2019-10213
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2019:2791

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Openshift Container Platform	4.1	All	All	All
Application	Redhat	Openshift Container Platform	4.2	All	All	All
Application	Redhat	Openshift Container Platform	4.1	All	All	All
Application	Redhat	Openshift Container Platform	4.2	All	All	All

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→