Bug 2262158 (CVE-2024-1139) - CVE-2024-1139 cluster-monitoring-operator: credentials leak

Keywords: Security

Status: NEW

Alias: CVE-2024-1139

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks: 2262168

TreeView+ depends on / blocked

Reported: 2024-01-31 20:53 UTC by Nick Tait

Modified: 2024-05-16 18:09 UTC (History)

CC List: 15 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2024:1887	0	None	None	None	2024-04-25 15:50:59 UTC
Red Hat Product Errata	RHSA-2024:2047	0	None	None	None	2024-05-02 16:37:33 UTC
Red Hat Product Errata	RHSA-2024:2782	0	None	None	None	2024-05-16 18:09:26 UTC

Nick Tait 2024-01-31 20:53:18 UTC Description

The below issue was reported to ProdSec by Simon Pasquier:

In OCP, the telemeter-client pod running in the
openshift-monitoring has an annotation containing the
cluster's pull secret
for the cloud.openshift.com and quay.io registries.

The cause of the bug is that we use the token string
concatenated with the
hash [2] instead of writing the token string to the hash
object and calling
Sum() with a nil slice.

The impact is that any user which can read the definition of
the
telemeter-client pod and/or deployment gets access to the pull
secret
token. Users with permissions from the cluster-reader
clusterrole already
have access to the original pull secret because they can read
the
"pull-secret" Secret in the openshift-config namespace.

The issue has been present since OCP 4.12 [3] [4].

[1] https://issues.redhat.com/browse/OCPBUGS-28650
[2]
https://github.com/openshift/cluster-monitoring-operator/blob/d45a3335c2bbada0948adef9fcba55c4e14fa1d7/pkg/manifests/manifests.go#L3135
[3] ~~https://bugzilla.redhat.com/show_bug.cgi?id=2114721~~
[4] https://github.com/openshift/cluster-monitoring-operator/pull/1747

errata-xmlrpc 2024-04-25 15:50:57 UTC Comment 5

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.15

Via RHSA-2024:1887 https://access.redhat.com/errata/RHSA-2024:1887

errata-xmlrpc 2024-05-02 16:37:32 UTC Comment 6

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.13

Via RHSA-2024:2047 https://access.redhat.com/errata/RHSA-

2024:2047

errata-xmlrpc 2024-05-16 18:09:25 UTC Comment 7

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.12

Via RHSA-2024:2782 https://access.redhat.com/errata/RHSA-2024:2782

Note

You need to log in before you can comment on or make changes to this bug.