Dashboard - Bug #47857

Feature # 47765 (New): mgr/dashboard: security improvements

mgr/dashboard: sensitive information stored in cleartext

10/14/2020 11:06 AM - Ernesto Puerta

Status:	New	**% Done:**	0%
Priority:	High		
Assignee:			
Category:	Security & Auth		
Target version:	v16.0.0		
Source:	other	**Affected Versions:**	
Tags:	security	**ceph-qa-suite:**	
Backport:	nautilus, octopus	**Pull request ID:**	
Regression:	No	**Crash signature (v1):**	
Severity:	2 - major	**Crash signature (v2):**	
Reviewed:			

Description

Description

The application stores sensitive information (i.e. usernames, passwords and access tokens) cleartext inside a RocksDB database. An attacker with read access to the database files could compromise the application and other systems.

Exploitation

The testing team identified a RocksDB instance in use by the Ceph Monitor daemon that contains sensitive data, such as S3 access and secret keys, usernames and passwords.
It was possible to easily obtain the data either by searching for ASCII strings in the database files or by using RocksDB command line tool to dump the database.

Recommendation

Either encrypt whole RocksDB or perform application-level encryption.

Caveat

Application level encryption still requires an encryption key to saved somewhere, which simply shifts the problem to where to securely store this key:

- Key-Value Store... un-encrypted. Same as original issue.
- Hardware Security Module (HSM), like a FIPS-140
- Remote key server (e.g.: Vault)

History

#1 - 04/15/2021 04:54 PM - Ernesto Puerta

- Project changed from mgr to Dashboard

- Category changed from 132 to General

#2 - 04/27/2021 02:06 PM - Ernesto Puerta

- Category changed from General to Security & Auth