rgw - Bug #39456

rgw: crypto: HMAC ctors cannot safely assert in (e.g.) FIPS mode

04/24/2019 08:48 PM - Matt Benjamin

Status:	Resolved	**% Done:**	0%
Priority:	Normal	**Spent time:**	0.00 hour
Assignee:	Matt Benjamin		
Category:			
Target version:			
Source:		**Affected Versions:**	
Tags:		**ceph-qa-suite:**	
Backport:	nautilus	**Pull request ID:**	27765
Regression:	No	**Crash signature (v1):**	
Severity:	3 - minor	**Crash signature (v2):**	
Reviewed:			

Description

Strategy to assert in constructors calling external crypto code--especially HMAC--can lead to an inappropriate abend/crash, for example, if the environment is RHEL FIPS and a stored key is too small per policy.

Matt

Related issues:

Copied to rgw - Backport #39676: nautilus: rgw: crypto: HMAC ctors cannot saf...	**Resolved**

History

#1 - 04/24/2019 09:09 PM - Matt Benjamin

- Pull request ID set to 27765

https://github.com/ceph/ceph/pull/27765

#2 - 04/25/2019 05:37 PM - Matt Benjamin

- Status changed from In Progress to 7

#3 - 05/08/2019 07:54 PM - Casey Bodley

- Status changed from 7 to Pending Backport

#4 - 05/10/2019 10:56 AM - Nathan Cutler

- Copied to Backport #39676: nautilus: rgw: crypto: HMAC ctors cannot safely assert in (e.g.) FIPS mode added

#5 - 06/15/2019 09:45 AM - Nathan Cutler

- Status changed from Pending Backport to Resolved