# rgw - Bug #52900

## segfault on FIPS enabled server as result of EVP_md5 disabled in openssl

10/12/2021 01:55 PM - Mark Kogan

| | | | |
|---|---|---|---|
| **Status:** | Pending Backport | **% Done:** | 0% |
| **Priority:** | Normal | **Spent time:** | 0.00 hour |
| **Assignee:** | Mark Kogan | | |
| **Category:** | | | |
| **Target version:** | | | |
| **Source:** | Q/A | **Affected Versions:** | |
| **Tags:** | | **ceph-qa-suite:** | |
| **Backport:** | pacific octopus | **Pull request ID:** | 43503 |
| **Regression:** | No | **Crash signature (v1):** | |
| **Severity:** | 2 - major | **Crash signature (v2):** | |
| **Reviewed:** | | | |

**Description**

reproduces in a vstart environment on

```
$ cat /etc/redhat-release
Red Hat Enterprise Linux release 8.4 (Ootpa)
```

with fips enabled:

```
$ sudo fips-mode-setup --enable
$ sudo systemctl reboot

$ sysctl crypto.fips_enabled
crypto.fips_enabled = 1
```

with the following flow:

```
./bin/radosgw-admin realm create --rgw-realm=gold
./bin/radosgw-admin zonegroup create --master --rgw-realm=gold --rgw-zonegroup=us --endpoints=http
://127.0.0.1:8000
./bin/radosgw-admin zone create --master --endpoints=http://127.0.0.1:8000 --rgw-realm=gold --rgw-
zonegroup=us --rgw-zone=us-east

# segfaults every time:
./bin/radosgw-admin period update --commit --rgw-realm=gold --rgw-zonegroup=us --rgw-zone=us-east
...
    -6> 2021-10-11T09:36:12.361+0000 7fa039ffb700 10 monclient: _finish_command 4 = mon:22 unparse
able JSON {"prefix": "osd pool set", "pool": "us-east.rgw.meta", "var": "recovery_priority": "5"}
    -5> 2021-10-11T09:36:12.361+0000 7fa102870c00  5 note: GC not initialized
    -4> 2021-10-11T09:36:12.362+0000 7fa102870c00  5 asok(0x55d0eaef2350) register_command sync tr
ace show hook 0x55d0eaf148e0
    -3> 2021-10-11T09:36:12.362+0000 7fa102870c00  5 asok(0x55d0eaef2350) register_command sync tr
ace history hook 0x55d0eaf148e0
    -2> 2021-10-11T09:36:12.362+0000 7fa102870c00  5 asok(0x55d0eaef2350) register_command sync tr
ace active hook 0x55d0eaf148e0
    -1> 2021-10-11T09:36:12.362+0000 7fa102870c00  5 asok(0x55d0eaef2350) register_command sync tr
ace active_short hook 0x55d0eaf148e0
```

```
    0> 2021-10-11T09:36:12.367+0000 7fa102870c00 -1 *** Caught signal (Segmentation fault) **
    in thread 7fa102870c00 thread_name:radosgw-admin

    ceph version 16.2.0-325-g0e34bb74700 (0e34bb74700060ebfaa22d99b7d2cdc037b28a57) pacific (stabl
e)
    1: /lib64/libpthread.so.0(+0x12b20) [0x7fa0f7b1fb20]
    NOTE: a copy of the executable, or `objdump -rdS <executable>` is needed to interpret this.
```

callstack in gdb:

```
multi-thre Thread 0x7ffff7fd82 In: ceph::crypto::ssl::OpenSSLDigest::Update
                                                                                L201  PC:
 0x7ffff4db8cac
(gdb) bt
#0  0x0000000000000000 in ?? ()
#1  0x00007ffff4db8cac in ceph::crypto::ssl::OpenSSLDigest::Update (this=0x7ffffffd80c0, input=0x2
ba2f70 "a122d7e2-650d-4488-b232-2fb1782e1342", length=36) at ../src/common/ceph_crypto.cc:201
#2  0x0000000001f95e9f in gen_short_zone_id (zone_id="a122d7e2-650d-4488-b232-2fb1782e1342") at ..
/src/rgw/rgw_zone.cc:1908
#3  0x0000000001f8b18a in RGWPeriodMap::update (this=0x7ffffffd9008, zonegroup=..., cct=0x29dd4c0)
 at ../src/rgw/rgw_zone.cc:1948
#4  0x0000000001f8c9ce in RGWPeriod::update (this=0x7ffffffd8fa8, dpp=0x2948d88 <dpp()::global_dpp
>, y=...) at ../src/rgw/rgw_zone.cc:1383
#5  0x00000000012b02e3 in update_period (realm_id="", realm_name="gold", period_id="", period_epoc
h="", commit=true, remote="", url="", opt_region=std::optional<std::string> [no contained value],
access="",
    secret="", formatter=0x2b8e750, force=false) at ../src/rgw/rgw_admin.cc:1776
#6  0x0000000001287f0f in main (argc=7, argv=0x7fffffffdec8) at ../src/rgw/rgw_admin.cc:5933
(gdb) f 1
#1  0x00007ffff4db8cac in ceph::crypto::ssl::OpenSSLDigest::Update (this=0x7ffffffd80c0, input=0x2
ba2f70 "a122d7e2-650d-4488-b232-2fb1782e1342", length=36) at ../src/common/ceph_crypto.cc:201
```

src/rgw/rgw_zone.cc is using 'EVP_md5' which is forbidden in FIPS

```
...
    static uint32_t gen_short_zone_id(const std::string zone_id)
    {
    unsigned char md5[CEPH_CRYPTO_MD5_DIGESTSIZE];
    MD5 hash;
...
```

**Related issues:**

| | |
|---|---|
| Duplicated by rgw - Bug #52799: Segmentation Fault in radosgw-admin period up... | **Duplicate** |
| Copied to rgw - Backport #53007: pacific: segfault on FIPS enabled server as ... | **New** |
| Copied to rgw - Backport #53008: octopus: segfault on FIPS enabled server as ... | **New** |

## History

#### #1 - 10/12/2021 03:13 PM - Mark Kogan

*- Pull request ID set to 43503*

created a PR (https://github.com/ceph/ceph/pull/43503) that activates the FIPS overriding mechanism in 2 locations (radosgw-admin & radosgw) following which it is possible to start a multisite environment with mstart/mrun/mrgw and perform s3cmd put/get/list/delete ops **without the segfault** above.

from a quick browse of the code, there seem to be another 29 locations where this is possibly necessary

```
git grep CEPH_CRYPTO_MD5_DIGESTSIZE | grep "E\]" | wc -l
29
```

#### #2 - 10/14/2021 02:25 PM - Casey Bodley

*- Duplicated by Bug #52799: Segmentation Fault in radosgw-admin period update --commit added*

#### #3 - 10/21/2021 02:34 PM - Casey Bodley

*- Status changed from In Progress to Pending Backport*

*- Backport set to pacific octopus*

#### #4 - 10/21/2021 02:35 PM - Backport Bot

*- Copied to Backport #53007: pacific: segfault on FIPS enabled server as result of EVP_md5 disabled in openssl added*

#### #5 - 10/21/2021 02:35 PM - Backport Bot

*- Copied to Backport #53008: octopus: segfault on FIPS enabled server as result of EVP_md5 disabled in openssl added*