RADOS - Bug #38827

valgrind: UninitCondition in ceph::crypto::onwire::AES128GCM_OnWireRxHandler::authenticated_decrypt_update_final()

03/20/2019 11:21 AM - Kefu Chai

Status:	Resolved	**% Done:**	0%
Priority:	High	**Spent time:**	0.00 hour
Assignee:	Radoslaw Zarzynski		
Category:	Correctness/Safety		
Target version:			
Source:		**Affected Versions:**	
Tags:		**ceph-qa-suite:**	
Backport:	nautilus	**Component(RADOS):**	
Regression:	No	**Pull request ID:**	28305
Severity:	3 - minor	**Crash signature (v1):**	
Reviewed:		**Crash signature (v2):**	

Description

```
<error>
  <unique>0x0</unique>
  <tid>12</tid>
  <threadname>msgr-worker-2</threadname>
  <kind>UninitCondition</kind>
  <what>Conditional jump or move depends on uninitialised value(s)</what>
  <stack>
    <frame>
      <ip>0x10430C7C</ip>
      <obj>/usr/lib64/libcrypto.so.1.0.2k</obj>
    </frame>
    <frame>
      <ip>0x1042CBD6</ip>
      <obj>/usr/lib64/libcrypto.so.1.0.2k</obj>
      <fn>EVP_DecryptFinal_ex</fn>
    </frame>
    <frame>
      <ip>0x5368F14</ip>
      <obj>/usr/lib64/ceph/libceph-common.so.0</obj>
      <fn>ceph::crypto::onwire::AES128GCM_OnWireRxHandler::authenticated_decrypt_update_final(ceph
::buffer::v14_2_0::list&amp;amp;&amp;amp;, unsigned int)</fn>
      <dir>/usr/src/debug/ceph-14.2.0-165-gba7267b/src/msg/async</dir>
      <file>crypto_onwire.cc</file>
      <line>267</line>
    </frame>
    <frame>
      <ip>0x5358151</ip>
      <obj>/usr/lib64/ceph/libceph-common.so.0</obj>
      <fn>ProtocolV2::handle_read_frame_epilogue_main(std::unique_ptr&amp;lt;ceph::buffer::v14_2_0::pt
r_node, ceph::buffer::v14_2_0::ptr_node::disposer&amp;gt;&amp;amp;&amp;amp;, int)</fn>
      <dir>/usr/src/debug/ceph-14.2.0-165-gba7267b/src/msg/async</dir>
      <file>ProtocolV2.cc</file>
      <line>1264</line>
    </frame>
...
```

/a/kchai-2019-03-20_05:45:48-rados-wip-kefu-testing-2019-03-20-1120-distro-basic-smithi/3751697/remote/smithi039/log/valgrind/m

on.a.log.gz

Related issues:	
Related to RADOS - Bug #44362: osd: uninitialized memory in sendmsg	**Can't reproduce**
Copied to RADOS - Backport #41534: nautilus: valgrind: UninitCondition in cep...	**Resolved**

History

#1 - 03/20/2019 11:24 AM - Kefu Chai

the test branch contains https://github.com/ceph/ceph/pull/27012

#2 - 03/20/2019 11:40 AM - Radoslaw Zarzynski

- Status changed from New to In Progress

- Assignee set to Radoslaw Zarzynski

#3 - 05/09/2019 04:22 PM - J. Eric Ivancich

- Priority changed from Normal to High

Is this being actively worked on?

How close are we to a fix on this?

I would like to make this a high priority bug, perhaps even urgent. This results in a lot of valgrind test failures on teuthology, thereby creating a lot of noise and adding to the workload of developers doing QA.

As an example, most of the failures in this teuthology run appear to be as a result of this bug:

http://pulpito.ceph.com/abhi-2019-05-07_13:40:09-rgw-wip-abhi-testing-2019-05-07-1047-distro-basic-smithi/

#4 - 05/16/2019 04:21 PM - Ali Maredia

The RGW verify suite has commented out the lines running valgrind on the mon.
https://github.com/ceph/ceph/pull/28155

Before this bug is resolved, that PR needs to be undone to ensure valgrind is being run on the mon in the rgw verify suite.

#5 - 05/28/2019 05:13 PM - Radoslaw Zarzynski

This bug looks like being duplicated by of http://tracker.ceph.com/issues/39449 which has been addressed with a pair of interconnected PRs:

- https://github.com/ceph/ceph/pull/27265 for ceph merged on Apr 2,
- https://github.com/ceph/teuthology/pull/1274 for teuthology on Apr 30.

The problem with the run mentioned by Eric (e.g. http://qa-proxy.ceph.com/teuthology/abhi-2019-05-07_13:40:09-rgw-wip-abhi-testing-2019-05-07-1047-distro-basic-smithi/3936972/remote/smithi031/log/valgrind/mon.b.log.gz) was that the bottom of the stack is:

```
    <!-- the msgr stuff -->
    <frame>
      <ip>0x5358BA4</ip>
      <obj>/usr/lib64/ceph/libceph-common.so.0</obj>
      <fn>EventCenter::process_events(unsigned int, std::chrono::duration&lt;unsigned long, std::ratio&lt;1l,
1000000000l&gt; &gt;*)</fn>
    </frame>
    <frame>
      <ip>0x535E8D6</ip>
```

```
      <obj>/usr/lib64/ceph/libceph-common.so.0</obj>
    </frame>
    <frame>
      <ip>0x55E4D5E</ip>
      <obj>/usr/lib64/ceph/libceph-common.so.0</obj>
    </frame>
    <frame>
      <ip>0x10756DD4</ip>
      <obj>/usr/lib64/libpthread-2.17.so</obj>
      <fn>start_thread</fn>
    </frame>
    <frame>
      <ip>0x118CBEAC</ip>
      <obj>/usr/lib64/libc-2.17.so</obj>
      <fn>clone</fn>
    </frame>
```

while in the whitelist we expect:

```
### the msgr stuff
fun:_ZN11EventCenter14process_eventsEjPNSt6chrono8durationImSt5ratioILl1ELl1000000000EEEE
fun:operator()
fun:_ZNSt17_Function_handlerIFvvEZN12NetworkStack10add_threadEjEUlvE_E9_M_invokeERKSt9_Any_data
fun:execute_native_thread_routine
fun:start_thread
fun:clone
```

It's a bit surprising as the unresolved symbols come from libceph-common. Anyway, I'm tuning the whitelist now.

#6 - 05/28/2019 05:43 PM - Radoslaw Zarzynski

Changeset: https://github.com/ceph/ceph/compare/master...rzarzynski:wip-bug-38827.

#7 - 05/28/2019 08:58 PM - Radoslaw Zarzynski

Scheduled a resurrected run for validation:
http://pulpito.front.sepia.ceph.com/rzarzynski-2019-05-28_20:56:45-rgw-wip-bug-38827-distro-basic-smithi/.

#8 - 05/29/2019 02:54 PM - Radoslaw Zarzynski

Second run (on slightly amended branch): http://pulpito.front.sepia.ceph.com/rzarzynski-2019-05-29_13:08:09-rgw-wip-bug-38827-distro-basic-smithi/

#9 - 05/29/2019 09:42 PM - Radoslaw Zarzynski

- Status changed from In Progress to Fix Under Review

https://github.com/ceph/ceph/pull/28305

#10 - 07/07/2019 02:48 AM - Kefu Chai

- Status changed from Fix Under Review to Resolved

#11 - 08/26/2019 07:33 PM - Casey Bodley

- Status changed from Resolved to Pending Backport

- Backport set to nautilus

seeing this in the rgw suite for nautilus runs, so tagging for backport of https://github.com/ceph/ceph/pull/28305

#12 - 08/27/2019 08:49 AM - Nathan Cutler

- Copied to Backport #41534: nautilus: valgrind: UninitCondition in ceph::crypto::onwire::AES128GCM_OnWireRxHandler::authenticated_decrypt_update_final() added

#13 - 08/27/2019 09:48 AM - Nathan Cutler

- Pull request ID set to 28305

#14 - 10/04/2019 09:07 AM - Nathan Cutler

- Status changed from Pending Backport to Resolved

While running with --resolve-parent, the script "backport-create-issue" noticed that all backports of this issue are in status "Resolved".

#15 - 03/04/2020 08:32 PM - Radoslaw Zarzynski

- Related to Bug #44362: osd: uninitialized memory in sendmsg added