# Ceph - Bug #19371

## monitor creation with IPv6 public network segfaults

03/24/2017 09:14 AM - Fabian Grünbichler

| | | | |
|---|---|---|---|
| **Status:** | Resolved | **Start date:** | 03/24/2017 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Fabian Grünbichler | **% Done:** | 0% |
| **Category:** | common | **Estimated time:** | 0.00 hour |
| **Target version:** | | **Spent time:** | 0.00 hour |
| **Source:** | Community (dev) | **Reviewed:** | |
| **Tags:** | | **Affected Versions:** | v0.39, v0.40, v0.41, v0.42, v0.43, v0.44, v0.45, v0.46, v0.47, v0.48, v0.49, v0.50, v0.51, v0.52a, v0.53a, v0.53b, v0.53c, v0.54a, v0.54b, v0.55a, v0.55b, v0.55c, v0.55d, v0.56, v0.57a, v0.57b, v0.57c, v0.58, v0.59, v0.60, v0.61 - Cuttlefish, v0.62a, v0.62b, v0.63, v0.64, v0.65, v0.66, v0.67 - Dumpling, v0.67rc, v0.67rc - continued, v0.68, v0.68 - continued, v0.69, v0.70, v0.71, v0.72 Emperor, v0.73, v0.74, v0.75, v0.76a, v0.76b, v0.77, 0.78, 0.79, 0.80rc, 0.80, v0.81, 0.82, 0.83, 0.83 cont., 0.84, 0.84 cont., 0.85, 0.85 cont., 0.86, 0.88, 0.89, 0.90, v.91, v.actually90, v.actually91, v0.92, v0.93 - Last Hammer Sprint, v0.94, v0.95, v9.0.2, v9.0.3, v9.0.4, v9.0.5, v9.0.6, v9.0.7, v9.0.8, v10.0.4, v0.80.10, v0.80.11, v0.80.12, v0.94.10, v0.94.11, v0.94.2, v0.94.3, v0.94.4, v0.94.5, v0.94.6, v0.94.7, v0.94.8, v0.94.9, v10.0.0, v10.1.1, v10.2.0, v10.2.1, v10.2.2, v10.2.3, v10.2.4, v10.2.5, v10.2.6, v10.2.7, v11.1.0, v11.2.1, v12.0.0, v9.1.1, v9.2.1, v9.2.2 |
| **Backport:** | hammer, jewel, kraken | **ceph-qa-suite:** | |
| **Regression:** | No | **Pull request ID:** | |
| **Severity:** | 4 - irritation | | |

**Description**

steps to reproduce:

1.) setup host using IPv6
2.) configure cluster and public network with IPv6 subnets in ceph.conf
3.) attempt to create a monitor
4.) ceph-mon --mkfs ... segfaults

the problematic code has been commited in 2011 before v0.39 - I haven't actually verified whether it is triggered that far back. it definitely triggers a segfault on Ceph Luminous (12.0.0)

the root cause is declaring a "struct sockaddr" in src/common/pick_address.cc find_ip_in_subnet_list, which is then first passed to parse_network and then to find_ip_in_subnet (both in src/common/ipaddr.cc). find_ip_in_subnet then casts the reference to sockaddr to one to sockaddr_in6 and assigns the IPv6 address. unfortunately, sockaddr is only 16 bytes big, so this assignment overwrites stuff on the stack.

note that the test cases don't catch this, as they only pass bigger structs casted to (sockaddr *) to parse_networks and find_ip_in_subnet when testing IPv6.

pull request will follow

| Related issues: | |
|---|---|
| Copied to Ceph - Backport #19463: hammer: monitor creation with IPv6 public n... | **Rejected** |
| Copied to Ceph - Backport #19464: jewel: monitor creation with IPv6 public ne... | **Resolved** |
| Copied to Ceph - Backport #19465: kraken: monitor creation with IPv6 public n... | **Resolved** |

## History

**#1 - 03/24/2017 09:24 AM - Fabian Grünbichler**

https://github.com/ceph/ceph/pull/14124

**#2 - 03/24/2017 12:25 PM - Kefu Chai**

*- Status changed from New to Need Review*

*- Assignee set to Fabian Grünbichler*

**#3 - 03/24/2017 12:58 PM - Kefu Chai**

*- Backport set to hammer, jewel, kraken*

**#4 - 04/01/2017 05:42 PM - Kefu Chai**

*- Status changed from Need Review to Pending Backport*

**#5 - 04/04/2017 12:41 PM - Nathan Cutler**

*- Copied to Backport #19463: hammer: monitor creation with IPv6 public network segfaults added*

**#6 - 04/04/2017 12:41 PM - Nathan Cutler**

*- Copied to Backport #19464: jewel: monitor creation with IPv6 public network segfaults added*

**#7 - 04/04/2017 12:42 PM - Nathan Cutler**

*- Copied to Backport #19465: kraken: monitor creation with IPv6 public network segfaults added*

**#8 - 09/04/2017 09:24 AM - Nathan Cutler**

*- Status changed from Pending Backport to Resolved*