Bug 1790725 - Libvirtd SIGSEGV on the condition that look up by target path '' when there is active pool without target path

Keywords:	Security ×
Status:	CLOSED ERRATA
Alias:	None
Product:	Red Hat Enterprise Linux Advanced Virtualization
Component:	libvirt
Version:	8.2
Hardware:	Unspecified
OS:	Unspecified
Priority:	high
Severity:	unspecified
Target Milestone:	rc
Target Release:	8.0
Assignee:	Cole Robinson
QA Contact:	~~gaojianan~~
Docs Contact:	
URL:	
Whiteboard:	
Depends On:	
Blocks:	~~CVE-2020-10703~~
TreeView+	depends on / blocked

Reported:	2020-01-14 02:37 UTC by Han Han
Modified:	2020-11-19 09:31 UTC (History)
CC List:	10 users (show)
Fixed In Version:	libvirt-6.0.0-1.el8
Doc Type:	If docs needed, set a value
Doc Text:	
Clone Of:	
Environment:	
Last Closed:	2020-05-05 09:55:17 UTC
Type:	Bug
Target Upstream Version:	
Dependent Products:	

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHBA-2020:2017	0	None	None	None	2020-05-05 09:56:58 UTC

Han Han 2020-01-14 02:37:29 UTC

Description

```
Description of problem:
As subject

Version-Release number of selected component (if applicable):
libvirt-5.10.0-2.module+el8.2.0+5274+60f836b5.x86_64

How reproducible:
100%

Steps to Reproduce:
1. Create a pool without target path, such as gluster pool
# cat /tmp/gluster-pool.xml
<pool type='gluster'>
  <name>mygluster</name>
  <uuid>65fcba04-5b13-bd93-cff3-52ce48e11ad8</uuid>
  <capacity unit='bytes'>0</capacity>
  <allocation unit='bytes'>0</allocation>
  <available unit='bytes'>0</available>
  <source>
    <host name='XX'/>
    <dir path='/'/>
    <name>gv</name>
  </source>
</pool>

# virsh pool-create /tmp/gluster-pool.xml
Pool mygluster created from /tmp/gluster-pool.xml

2. Try lookup storage pool with target path '' by readonly connection
#! /usr/bin/python3
import libvirt
conn=libvirt.openReadOnly('qemu+ssh://root.84.11/system')
conn.storagePoolLookupByTargetPath('')

# abrt-cli ls
id 3f82872a3321aa5ee63161d02bf714e983e00968
reason:         __strcmp_sse2(): libvirtd killed by SIGSEGV
time:           Tue 14 Jan 2020 10:16:23 AM CST
cmdline:        /usr/sbin/libvirtd --timeout 120
package:        libvirt-daemon-5.10.0-2.module+el8.2.0+5274+60f836b5
uid:            0 (root)
count:          1
Directory:      /var/spool/abrt/ccpp-2020-01-14-10:16:23-3035
Run 'abrt-cli report /var/spool/abrt/ccpp-2020-01-14-10:16:23-3035' for creating a case in Red Hat Customer Portal

Backtrace:
#0  0x00007ff55604ebbe in __strcmp_sse2 () at ../sysdeps/x86_64/strcmp.S:174
#1  0x00007ff538c9f990 in storagePoolLookupByTargetPathCallback (opaque=0x7ff53003c400, obj=0x7ff53c0039a0) at ../../src/storage/storage_driver.c:1718
#2  0x00007ff538c9f990 in storagePoolLookupByTargetPathCallback (obj=0x7ff53c0039a0, opaque=0x7ff53003c400) at ../../src/storage/storage_driver.c:1708
#3  0x00007ff559cc548f in virStoragePoolObjListSearchCb (payload=0x7ff53c0039a0, name=<optimized out>, opaque=0x7ff542050780) at
../../src/conf/virstorageobj.c:488
#4  0x00007ff559be41c5 in virHashSearch (name=<optimized out>, data=<optimized out>, iter=<optimized out>, ctable=<optimized out>) at
../../src/util/virhash.c:745
#5  0x00007ff559be41c5 in virHashSearch
    (ctable=0x7ff4e40f6450, iter=iter@entry=0x7ff559cc5470 <virStoragePoolObjListSearchCb>, data=data@entry=0x7ff542050780, name=name@entry=0x0)
    at ../../src/util/virhash.c:729
#6  0x00007ff559cc66f0 in virStoragePoolObjListSearch
    (pools=0x7ff4e40f9a50, searcher=searcher@entry=0x7ff538c9f960 <storagePoolLookupByTargetPathCallback>, opaque=opaque@entry=0x7ff53003c400)
    at ../../src/conf/virstorageobj.c:517
#7  0x00007ff538c9e676 in storagePoolLookupByTargetPath (conn=0x7ff53c002530, path=0x7ff53003c2d0 "") at ../../src/storage/storage_driver.c:1735
#8  0x00007ff559df9595 in virStoragePoolLookupByTargetPath (conn=0x7ff53c002530, path=0x7ff53003c2d0 "") at ../../src/libvirt-storage.c:531
#9  0x0000555bb8828e1c in remoteDispatchStoragePoolLookupByTargetPath
    (server=0x555bb9a62950, msg=0x555bb9a9b440, args=0x7ff530034de0, ret=0x7ff53004f7d0, rerr=0x7ff5420508e0, client=0x555bb9abf640)
    at ./remote/remote_daemon_dispatch_stubs.h:17566
#10 0x0000555bb8828e1c in remoteDispatchStoragePoolLookupByTargetPathHelper
    (server=0x555bb9a62950, client=0x555bb9abf640, msg=0x555bb9a9b440, rerr=0x7ff5420508e0, args=0x7ff530034de0, ret=0x7ff53004f7d0)
    at ./remote/remote_daemon_dispatch_stubs.h:17547
#11 0x00007ff559d0f169 in virNetServerProgramDispatchCall (msg=0x555bb9a9b440, client=0x555bb9abf640, server=0x555bb9a62950, prog=0x555bb9aa0da0)
    at ../../src/rpc/virnetserverprogram.c:430
#12 0x00007ff559d0f169 in virNetServerProgramDispatch (prog=0x555bb9aa0da0, server=server@entry=0x555bb9a62950, client=0x555bb9abf640, msg=0x555bb9a9b440)
    at ../../src/rpc/virnetserverprogram.c:302
#13 0x00007ff559d1430c in virNetServerProcessMsg (msg=<optimized out>, prog=<optimized out>, client=<optimized out>, srv=0x555bb9a62950)
    at ../../src/rpc/virnetserver.c:136
#14 0x00007ff559d1430c in virNetServerHandleJob (jobOpaque=<optimized out>, opaque=0x555bb9a62950) at ../../src/rpc/virnetserver.c:153
#15 0x00007ff559c33800 in virThreadPoolWorker (opaque=opaque@entry=0x555bb9a46a80) at ../../src/util/virthreadpool.c:163
```

```
#16 0x00007ff559c32b8c in virThreadHelper (data=<optimized out>) at ../../src/util/virthread.c:196
#17 0x00007ff5563882de in start_thread (arg=<optimized out>) at pthread_create.c:486
#18 0x00007ff5560b9e83 in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:95
```

Actual results:
As above

Expected results:
no SIGSEGV

Additional info:
A patch has been committed to fix it in libvirt-6.0

```
commit dfff16a7c2
Author: Yi Li <yili>
Date:   Sat Dec 21 08:33:33 2019 +0800

    storage: Fix daemon crash on lookup storagepool by targetpath

    Causing a crash when storagePoolLookupByTargetPath beacuse of
    Some types of storage pool have no target elements.
    Use STREQ_NULLABLE instead of STREQ
    Avoids segfaults when using NULL arguments.

    Core was generated by `/usr/sbin/libvirtd'.
    Program terminated with signal 11, Segmentation fault.
    (gdb) bt
    0  0x0000ffff9e951388 in strcmp () from /lib64/libc.so.6
    1  0x0000ffff92103e9c in storagePoolLookupByTargetPathCallback (
        obj=0xffff7009aab0, opaque=0xffff801058b0) at storage/storage_driver.c:1649
    2  0x0000ffff9f2c52a4 in virStoragePoolObjListSearchCb (
        payload=0xffff801058b0, name=<optimized out>, opaque=<optimized out>)
        at conf/virstorageobj.c:476
    3  0x0000ffff9f1f2f7c in virHashSearch (ctable=0xffff800f4f60,
        iter=iter@entry=0xffff9f2c5278 <virStoragePoolObjListSearchCb>,
        data=data@entry=0xffff95af7488, name=name@entry=0x0) at util/virhash.c:696
    4  0x0000ffff9f2c64f0 in virStoragePoolObjListSearch (pools=0xffff800f2ce0,
        searcher=searcher@entry=0xffff92103e68 <storagePoolLookupByTargetPathCallback>,
         opaque=<optimized out>) at conf/virstorageobj.c:505
    5  0x0000ffff92101f54 in storagePoolLookupByTargetPath (conn=0xffff5c0009f0,
    path=0xffff7009a850 "/vms/images") at storage/storage_driver.c:1672

    Reviewed-by: Cole Robinson <crobinso>
    Signed-off-by: Yi Li <yili>
```

Add security flag since unprivileged user could exploit it to make libvirtd down.
Reproduced on RHEL7.8 libvirt-4.5.0-28.el7.x86_64.
Please check if it should be fixed on all the RHEL7 and RHEL8 z stream.

Han Han 2020-01-14 02:39:19 UTC Comment 1

Step2 should be a locale connection:
conn=libvirt.openReadOnly('qemu+ssh:///system')

Han Han 2020-02-04 02:27:09 UTC Comment 3

Hi Cole,
Since it can cause libvirtd segment fault by readonly connection, do we need to request a CVE and clone it to z stream versions of RHEL7 and RHEL8?

~~gaojianan~~ 2020-02-05 06:23:33 UTC Comment 6

Verified on :
libvirt-6.0.0-2.virtcov.el8.x86_64

Step:
1.Create different kinds of pool without target element:
  iscsi-direct pool:

```
<pool type="iscsi-direct">
  <name>virtimages</name>
  <source>
    <host name="10.66.85.243"/>
    <device path="iqn.2020-01.com.virttest:blockdev-pool.target6"/>
            <initiator>
      <iqn name="iqn.2013-06.com.example:iscsi-initiator"/>
    </initiator>
  </source>
</pool>
```

 gluster pool:

```
<pool type='gluster'>
  <name>mygluster</name>
  <uuid>65fcba04-5b13-bd93-cff3-52ce48e11ad8</uuid>
  <capacity unit='bytes'>0</capacity>
  <allocation unit='bytes'>0</allocation>
  <available unit='bytes'>0</available>
  <source>
    <host name='$ip'/>
    <dir path='/'/>
    <name>jgao-vol2</name>
  </source>
</pool>
```

2.Try lookup storage pool with target path '' by readonly connection:

```
#!/usr/bin/python3
import libvirt
conn=libvirt.openReadOnly('qemu+ssh:///system')
conn.storagePoolLookupByTargetPath('')
ret = conn.storagePoolLookupByTargetPath('')
print(ret)
```

No SIGSEGV found,work as expected

errata-xmlrpc 2020-05-05 09:55:17 UTC Comment 9

Since the problem described in this bug report should be
resolved in a recent advisory, it has been closed with a
resolution of ERRATA.

For information on the advisory, and where to find the updated
files, follow the link below.

If the solution does not work for you, open a new bug report.

https://access.redhat.com/errata/RHBA-2020:2017

Note

You need to log in before you can comment on or make changes to this bug.