SELinux - Bug #13357

Passenger wants to exec lsof after crash

01/25/2016 08:45 AM - Lukas Zapletal

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	General Foreman		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

If there is a crash during Foreman startup (raise a bug in engine.rb or initializer), Passenger tries to sniff around on the system to create "Dump information" that then appear in httpd error log. This is not allowed in the current policy resulting in:

```
### Backtraces
Thread 'Main thread' (0x7f24ae8bc740, LWP 16927):
     in 'void Server::mainLoop()' (Main.cpp:540)

Thread 'MultiLibeio dispatcher' (0x7f24ae8ba700, LWP 16927):
     (empty)

Thread 'Pool analytics collector' (0x7f24ae8a9700, LWP 16927):
     in 'static void Passenger::ApplicationPool2::Pool::collectAnalytics(Passenger::ApplicationPoo
l2::PoolPtr)' (Pool.h:682)

Thread 'Pool garbage collector' (0x7f24ae868700, LWP 16927):
     in 'static void Passenger::ApplicationPool2::Pool::garbageCollect(Passenger::ApplicationPool2
::PoolPtr)' (Pool.h:549)

Thread 'Thread #2' (0x7f24ad8af700, LWP 16927):
     (empty)

Thread 'MessageServer thread' (0x7f24ae827700, LWP 16927):
     in 'void Passenger::MessageServer::mainLoop()' (MessageServer.h:558)

Thread 'Pool event loop' (0x7f24ad0ae700, LWP 16927):
     (empty)

Thread 'Request event loop' (0x7f24ac8ad700, LWP 16927):
     (empty)

Thread 'PipeWatcher: PID 16955 stdout, fd 25' (0x7f24ae732700, LWP 16953):
     in 'void Passenger::ApplicationPool2::PipeWatcher::threadMain()' (Implementation.cpp:1246)
     in 'static void Passenger::ApplicationPool2::PipeWatcher::threadMain(boost::shared_ptr<Passen
ger::ApplicationPool2::PipeWatcher>)' (Implementation.cpp:1227)

Thread 'PipeWatcher: PID 16955 stderr, fd 26' (0x7f24ae806700, LWP 16953):
     in 'void Passenger::ApplicationPool2::PipeWatcher::threadMain()' (Implementation.cpp:1246)
     in 'static void Passenger::ApplicationPool2::PipeWatcher::threadMain(boost::shared_ptr<Passen
ger::ApplicationPool2::PipeWatcher>)' (Implementation.cpp:1227)

Thread 'PipeWatcher: PID 17059 stdout, fd 27' (0x7f24ac0ac700, LWP 16953):
     in 'void Passenger::ApplicationPool2::PipeWatcher::threadMain()' (Implementation.cpp:1246)
     in 'static void Passenger::ApplicationPool2::PipeWatcher::threadMain(boost::shared_ptr<Passen
ger::ApplicationPool2::PipeWatcher>)' (Implementation.cpp:1227)

-------------------------------------
```

```
[ pid=16927 ] Open files and file descriptors:
lsof: WARNING: can't stat() hugetlbfs file system /dev/hugepages
      Output information may be incomplete.
lsof: WARNING: can't stat() nfsd file system /proc/fs/nfsd
      Output information may be incomplete.
lsof: WARNING: can't stat() cgroup file system /sys/fs/cgroup/systemd
      Output information may be incomplete.
lsof: WARNING: can't stat() cgroup file system /sys/fs/cgroup/cpu,cpuacct
      Output information may be incomplete.
lsof: WARNING: can't stat() cgroup file system /sys/fs/cgroup/freezer
      Output information may be incomplete.
lsof: WARNING: can't stat() cgroup file system /sys/fs/cgroup/net_cls
      Output information may be incomplete.
lsof: WARNING: can't stat() cgroup file system /sys/fs/cgroup/perf_event
      Output information may be incomplete.
lsof: WARNING: can't stat() cgroup file system /sys/fs/cgroup/hugetlb
      Output information may be incomplete.
lsof: WARNING: can't stat() cgroup file system /sys/fs/cgroup/devices
      Output information may be incomplete.
lsof: WARNING: can't stat() cgroup file system /sys/fs/cgroup/memory
      Output information may be incomplete.
lsof: WARNING: can't stat() cgroup file system /sys/fs/cgroup/blkio
      Output information may be incomplete.
lsof: WARNING: can't stat() cgroup file system /sys/fs/cgroup/cpuset
      Output information may be incomplete.
lsof: WARNING: can't stat() pstore file system /sys/fs/pstore
      Output information may be incomplete.
lsof: WARNING: can't stat() configfs file system /sys/kernel/config
      Output information may be incomplete.
lsof: WARNING: can't stat() debugfs file system /sys/kernel/debug
      Output information may be incomplete.
lsof: WARNING: can't stat() tmpfs file system /run/user/0
      Output information may be incomplete.
lsof: WARNING: can't stat() rpc_pipefs file system /var/lib/nfs/rpc_pipefs
      Output information may be incomplete.
lsof: WARNING: can't stat() tmpfs file system /run/user/990
      Output information may be incomplete.

----
time->Sun Jan 24 07:43:32 2016
type=SYSCALL msg=audit(1453639412.380:1062): arch=c000003e syscall=10 success=no exit=-13 a0=7fc6a
8ef6000 a1=1000 a2=5 a3=7ffd4c1a9f50 items=0 ppid=26926 pid=26927 auid=4294967295 uid=990 gid=986
euid=990 suid=990 fsuid=990 egid=986 sgid=986 fsgid=986 tty=(none) ses=4294967295 comm="ruby" exe=
"/opt/rh/ruby193/root/usr/bin/ruby" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1453639412.380:1062): avc:  denied  { execmem } for  pid=26927 comm="ruby" scon
text=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
----
time->Sun Jan 24 07:43:33 2016
type=SYSCALL msg=audit(1453639413.632:1063): arch=c000003e syscall=4 success=no exit=-13 a0=7ffdc3
f78a50 a1=7ffdc3f79a60 a2=7ffdc3f79a60 a3=7ffdc3f78790 items=0 ppid=27063 pid=27065 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="lsof" ex
e="/usr/sbin/lsof" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1453639413.632:1063): avc:  denied  { getattr } for  pid=27065 comm="lsof" path
="/dev/hugepages" dev="hugetlbfs" ino=10248 scontext=system_u:system_r:passenger_t:s0 tcontext=sys
tem_u:object_r:hugetlbfs_t:s0 tclass=dir
----
time->Sun Jan 24 07:43:33 2016
type=SYSCALL msg=audit(1453639413.632:1064): arch=c000003e syscall=4 success=no exit=-13 a0=7ffdc3
f78a50 a1=7ffdc3f79a60 a2=7ffdc3f79a60 a3=7ffdc3f78790 items=0 ppid=27063 pid=27065 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="lsof" ex
e="/usr/sbin/lsof" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1453639413.632:1064): avc:  denied  { getattr } for  pid=27065 comm="lsof" path
="/proc/fs/nfsd" dev="nfsd" ino=1 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:obje
ct_r:nfsd_fs_t:s0 tclass=dir
----
time->Sun Jan 24 07:43:33 2016
type=SYSCALL msg=audit(1453639413.632:1065): arch=c000003e syscall=4 success=no exit=-13 a0=7ffdc3
```

```
f78a50 a1=7ffdc3f79a60 a2=7ffdc3f79a60 a3=7ffdc3f78790 items=0 ppid=27063 pid=27065 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="lsof" ex
e="/usr/sbin/lsof" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1453639413.632:1065): avc:  denied  { getattr } for  pid=27065 comm="lsof" path
="/sys/fs/cgroup/systemd" dev="cgroup" ino=6407 scontext=system_u:system_r:passenger_t:s0 tcontext
=system_u:object_r:cgroup_t:s0 tclass=dir
----
time->Sun Jan 24 07:43:33 2016
type=SYSCALL msg=audit(1453639413.633:1066): arch=c000003e syscall=4 success=no exit=-13 a0=7ffdc3
f78a50 a1=7ffdc3f79a60 a2=7ffdc3f79a60 a3=7ffdc3f78790 items=0 ppid=27063 pid=27065 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="lsof" ex
e="/usr/sbin/lsof" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1453639413.633:1066): avc:  denied  { getattr } for  pid=27065 comm="lsof" path
="/sys/fs/cgroup/cpu,cpuacct" dev="cgroup" ino=6433 scontext=system_u:system_r:passenger_t:s0 tcon
text=system_u:object_r:cgroup_t:s0 tclass=dir
----
time->Sun Jan 24 07:43:33 2016
type=SYSCALL msg=audit(1453639413.633:1067): arch=c000003e syscall=4 success=no exit=-13 a0=7ffdc3
f78a50 a1=7ffdc3f79a60 a2=7ffdc3f79a60 a3=7ffdc3f78790 items=0 ppid=27063 pid=27065 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="lsof" ex
e="/usr/sbin/lsof" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1453639413.633:1067): avc:  denied  { getattr } for  pid=27065 comm="lsof" path
="/sys/fs/cgroup/freezer" dev="cgroup" ino=6453 scontext=system_u:system_r:passenger_t:s0 tcontext
=system_u:object_r:cgroup_t:s0 tclass=dir
----
time->Sun Jan 24 07:43:33 2016
type=SYSCALL msg=audit(1453639413.633:1068): arch=c000003e syscall=4 success=no exit=-13 a0=7ffdc3
f78a50 a1=7ffdc3f79a60 a2=7ffdc3f79a60 a3=7ffdc3f78790 items=0 ppid=27063 pid=27065 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="lsof" ex
e="/usr/sbin/lsof" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1453639413.633:1068): avc:  denied  { getattr } for  pid=27065 comm="lsof" path
="/sys/fs/cgroup/net_cls" dev="cgroup" ino=6462 scontext=system_u:system_r:passenger_t:s0 tcontext
=system_u:object_r:cgroup_t:s0 tclass=dir
----
time->Sun Jan 24 07:43:33 2016
type=SYSCALL msg=audit(1453639413.633:1069): arch=c000003e syscall=4 success=no exit=-13 a0=7ffdc3
f78a50 a1=7ffdc3f79a60 a2=7ffdc3f79a60 a3=7ffdc3f78790 items=0 ppid=27063 pid=27065 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="lsof" ex
e="/usr/sbin/lsof" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1453639413.633:1069): avc:  denied  { getattr } for  pid=27065 comm="lsof" path
="/sys/fs/cgroup/perf_event" dev="cgroup" ino=6472 scontext=system_u:system_r:passenger_t:s0 tcont
ext=system_u:object_r:cgroup_t:s0 tclass=dir
----
time->Sun Jan 24 07:43:33 2016
type=SYSCALL msg=audit(1453639413.633:1070): arch=c000003e syscall=4 success=no exit=-13 a0=7ffdc3
f78a50 a1=7ffdc3f79a60 a2=7ffdc3f79a60 a3=7ffdc3f78790 items=0 ppid=27063 pid=27065 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="lsof" ex
e="/usr/sbin/lsof" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1453639413.633:1070): avc:  denied  { getattr } for  pid=27065 comm="lsof" path
="/sys/fs/cgroup/hugetlb" dev="cgroup" ino=6481 scontext=system_u:system_r:passenger_t:s0 tcontext
=system_u:object_r:cgroup_t:s0 tclass=dir
----
time->Sun Jan 24 07:43:33 2016
type=SYSCALL msg=audit(1453639413.633:1071): arch=c000003e syscall=4 success=no exit=-13 a0=7ffdc3
f78a50 a1=7ffdc3f79a60 a2=7ffdc3f79a60 a3=7ffdc3f78790 items=0 ppid=27063 pid=27065 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="lsof" ex
e="/usr/sbin/lsof" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1453639413.633:1071): avc:  denied  { getattr } for  pid=27065 comm="lsof" path
="/sys/fs/cgroup/devices" dev="cgroup" ino=6494 scontext=system_u:system_r:passenger_t:s0 tcontext
=system_u:object_r:cgroup_t:s0 tclass=dir
----
time->Sun Jan 24 07:43:33 2016
type=SYSCALL msg=audit(1453639413.633:1072): arch=c000003e syscall=4 success=no exit=-13 a0=7ffdc3
f78a50 a1=7ffdc3f79a60 a2=7ffdc3f79a60 a3=7ffdc3f78790 items=0 ppid=27063 pid=27065 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="lsof" ex
e="/usr/sbin/lsof" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1453639413.633:1072): avc:  denied  { getattr } for  pid=27065 comm="lsof" path
```

```
="/sys/fs/cgroup/memory" dev="cgroup" ino=6506 scontext=system_u:system_r:passenger_t:s0 tcontext=
system_u:object_r:cgroup_t:s0 tclass=dir
----
time->Sun Jan 24 07:43:33 2016
type=SYSCALL msg=audit(1453639413.633:1073): arch=c000003e syscall=4 success=no exit=-13 a0=7ffdc3
f78a50 a1=7ffdc3f79a60 a2=7ffdc3f79a60 a3=7ffdc3f78790 items=0 ppid=27063 pid=27065 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="lsof" ex
e="/usr/sbin/lsof" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1453639413.633:1073): avc:  denied  { getattr } for  pid=27065 comm="lsof" path
="/sys/fs/cgroup/blkio" dev="cgroup" ino=6541 scontext=system_u:system_r:passenger_t:s0 tcontext=s
ystem_u:object_r:cgroup_t:s0 tclass=dir
----
time->Sun Jan 24 07:43:33 2016
type=SYSCALL msg=audit(1453639413.633:1074): arch=c000003e syscall=4 success=no exit=-13 a0=7ffdc3
f78a50 a1=7ffdc3f79a60 a2=7ffdc3f79a60 a3=7ffdc3f78790 items=0 ppid=27063 pid=27065 auid=429496729
5 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="lsof" ex
e="/usr/sbin/lsof" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1453639413.633:1074): avc:  denied  { getattr } for  pid=27065 comm="lsof" path
="/sys/fs/cgroup/cpuset" dev="cgroup" ino=6577 scontext=system_u:system_r:passenger_t:s0 tcontext=
system_u:object_r:cgroup_t:s0 tclass=dir
----
... many similar ...

#============= passenger_t ==============
allow passenger_t NetworkManager_var_run_t:sock_file getattr;
allow passenger_t cgroup_t:dir getattr;
allow passenger_t configfs_t:dir getattr;
allow passenger_t device_t:sock_file write;
allow passenger_t fixed_disk_device_t:blk_file getattr;
allow passenger_t gssproxy_var_lib_t:dir search;
allow passenger_t gssproxy_var_run_t:sock_file getattr;
allow passenger_t httpd_var_run_t:sock_file getattr;
allow passenger_t hugetlbfs_t:dir getattr;
allow passenger_t init_var_run_t:sock_file getattr;
allow passenger_t lvm_var_run_t:sock_file getattr;
allow passenger_t nfsd_fs_t:dir getattr;
allow passenger_t pstore_t:dir getattr;
allow passenger_t rpcbind_var_run_t:sock_file getattr;
allow passenger_t self:process execmem;
allow passenger_t system_dbusd_var_run_t:sock_file getattr;
allow passenger_t udev_var_run_t:sock_file getattr;
allow passenger_t var_lib_nfs_t:dir search;

#============= policykit_t ==============
allow policykit_t device_t:sock_file write;

#============= postfix_pickup_t ==============
allow postfix_pickup_t device_t:sock_file write;

#============= syslogd_t ==============
allow syslogd_t unlabeled_t:file { read open };
allow syslogd_t var_run_t:file read;
```

I am keeping this bug opened just for the record, root cause needs to be fixed in this case (this was OpenSCAP initialization Ruby FFI error) in order to silence these errors. We might consider allowing calling "lsof" on those files, I am not sure how safe this is.

Related issues:

Related to SELinux - Bug #22028: Passenger denials during restart	**Duplicate**	**12/19/2017**

History

#1 - 05/30/2018 09:01 AM - Lukas Zapletal

- Related to Bug #22028: Passenger denials during restart added

#2 - 05/30/2018 09:02 AM - Lukas Zapletal

- Status changed from New to Closed

We will not allow this in our policy.