New issue

Jump to bottom

Reduce leakage of disposable VM content and history into dom0 filesystem #4972

Open **brendanhoar** opened this issue on Apr 12, 2019 · 18 comments

Labels C: other help wanted P: default privacy T: enhancement

Considerable information about the history of disposable VM usage, as well as some contents of data from inside disposable VM leaks into the filesystem of dom0 and in most cases, survives reboots.

In particular, the leakage into the xfwm4-*.state files (and lack of cleanup) is particular disturbing.

e.g. in dom0
rm disp_files.txt # if exists
rm disp_contents.txt # if exists
sudo grep -rn '/' -e 'disp[0-9]' --exclude-dir={dev,proc,sys} | sort > disp_contents.txt
sudo find / -name *disp[0-9]* | sort > disp_files.txt # matches references to disposable VM names in filenames

Some findings on files related to disposable VMs (via disp_files.txt):

1. snapshots/volatile volumes for disposable VMs that were not shutdown correctly in the past (found in /dev/qubes_dom0/ and /dev/mapper/)
2. xml config files for the same in /etc/libvirt/libxl/ and /run/libvirt/libxl/
3. appmenus for the same in /home/admin/.local/share/
4. qrexec files for the same in /run/qubes/
5. qubes.db pid and sock files for the same in /run/qubes/
6. linux mapper links for the same in /run/udev/links/{\x2fmapper,\x2fqubes_dom0}/
7. directories for the above in /var/lib/qubes/appvms/
8. libxl logs for every(!!!) disposable VM ever run in this Qubes install in /var/log/libvirt/libxl/
9. qubes logs for every(!!!) disposable VM ever run in this Qubes install in /var/log/qubes/
10. xen console logs for every(!!!!) disposable VM ever run in this Qubes install in /var/log/xen/console/

Some finding related to files *containing* references to disposable VMs in dom0 (via disp_contents.txt):

1. Current and many historical disposable VM references are found in files in /run/udev/data/b253* files/nodes.
2. xfwm4*.state files in /home/admin/.cache/sessions/ contains *many references* to disposable VM *WINDOW TITLES* (application names, web site names, etc.) since the installation of the Qubes install (as well as current session).
3. .xsession-errors* in ~ reference many disposable VM names
4. /home/admin/.config/pulse/{guid}-stream-volumes.tdb a binary file appears to have 0..n matches on disp[0-9].
5. /etc/lvm/backup/qubes_dom0 has current disp VM names plus some that weren't shutdown cleanly.
6. /etc/lvm/backup/qubes_dom0_* files have historical disp VM names.
7. /var/log/qubes/qubes.log* references historical disp VM names.
8. The systemd journal has a ton of historical disp VM references.

11. /var/lib/xen/userdata* contains a lot of historical disp VM references.
12. /var/lib/logrotate/logrotate.status contains a lot of historical disp VM references.

Describe the solution you'd like

1. Triage of types of data leaking into dom0.
2. Based on types of data, develop a Qubes policy on eliminating, reducing, cleaning or ignoring the leaked data.
3. Based on type/policy, institute efforts to reduce the content stored into dom0 (at all vs. short term vs long term).

Where is the value to a user, and who might that user be?
All users who may want the historical content of the disposable VM usage not to be memorialized. Journalists, security researchers, etc.

Describe alternatives you've considered
None appear to cover 100% of use cases. Perhaps TAILS in an HVM might reduce it the most.

Additional context

Relevant documentation you've consulted

Related, non-duplicate issues
#3504 (similar, but does not provide a focus on specific leakage into dom0)
#4408 (anti-forensics on swap files only)
#1819 (anti-forensics request only covers the block devices for the VM)
#1293 (similar to 1819)
#3360 (specific to dom0 logging only)
#2024 (emulating Tails' approach, dom0 leakage still possible)

❤️ 3

brendanhoar added P: default T: enhancement labels on Apr 12, 2019

marmarek commented on Apr 12, 2019 Member

Thanks for the research!

Some of those indeed needs improvements. But note that majority of this points in practice only give information about the name of disposable VM, which isn't really much. It will leak how much you use disposable VMs, but not really what you do inside. And since pool of available dispXXX names is relatively small (10k), those names aren't really unique to the specific qubes instance.

andrewdavidwong added this to the **Far in the future** milestone on Apr 13, 2019

cfcs commented on Apr 13, 2019

I'm personally quite bothered by the ctrl-shift-c copy-paste mechanism writing to disk :-/
It's

1. annoying when you run out of disk space
2. potentially not what you wanted if you're using an encrypted password manager and frequently copy-paste passwords.

h01ger commented on Apr 13, 2019 via email

> On Sat, Apr 13, 2019 at 03:55:40AM -0700, cfcs wrote:
> I'm personally quite bothered by the ctrl-shift-c copy-paste mechanism writing to disk :-/

eeks :(where to exactly?

(and thank you for pointing this out.)

…

marmarek commented on Apr 13, 2019 Member

> I'm personally quite bothered by the ctrl-shift-c copy-paste mechanism writing to disk :-/

Not really. It is in /var/run/qubes, which is on tmpfs. With a little caveat: swap

👍 1

cfcs commented on Apr 13, 2019

Ah, fair enough! I was just getting errors that "out of disk space," but that must have been from the `tmpfs` and the actual problem being out of (provisioned) memory :)

h01ger commented on Apr 13, 2019 via email

> On Sat, Apr 13, 2019 at 04:40:37AM -0700, Marek Marczykowski-Górecki wrote:
> Not really. It is in /var/run/qubes, which is on tmpfs. With a little caveat: [swap](#977)

thanks for clarifying!

brendanhoar commented on Apr 14, 2019 Author

@andrewdavidwong - FYI, I don't think this one sub-item should be tagged minor: "xfwm4*.state files in /home/admin/.cache/sessions/ contains many references to disposable VM WINDOW TITLES (application names, web site names, etc.) since the installation of the Qubes install (as well as current session)."

👍 1

andrewdavidwong commented on Apr 14, 2019 Member

> @andrewdavidwong - FYI, I don't think this one sub-item should be tagged minor: "xfwm4*.state files in /home/admin/.cache/sessions/ contains many references to disposable VM WINDOW TITLES (application names, web site names, etc.) since the installation of the Qubes install (as well as current session)."

Sure, but what do you mean by "sub-item"?

andrewdavidwong added P: default and removed P: minor labels on Apr 14, 2019

unman commented on Apr 15, 2019 Member

For what it's worth, I dont think that KDE stores anything like the same amount of state information as Xfce.

brendanhoar commented on Apr 15, 2019 • edited Author

> > @andrewdavidwong - FYI, I don't think this one sub-item should be tagged minor: "xfwm4*.state files in /home/admin/.cache/sessions/ contains many references to disposable VM WINDOW TITLES (application names, web site names, etc.) since the installation of the Qubes install (as well as current session)."
> > Sure, but what do you mean by "sub-item"?

There were 22 items in the original issue (10 in section 1, 12 in section 2).

In particular, Section 2 (contents of files), Item 2 (xfwm4*.state files). Search for xfwm4.

Brendan

andrewdavidwong commented on Apr 16, 2019 Member

> > > @andrewdavidwong - FYI, I don't think this one sub-item should be tagged

> > names, etc.) since the installation of the Qubes install (as well as current session).
> > Sure, but what do you mean by "sub-item"?
>
> There were 22 items in the original issue (10 in section 1, 12 in section 2).
>
> In particular, Section 2 (contents of files), Item 2 (xfwm4*.state files). Search for xfwm4.
>
> Brendan

Yes, but the priority applies to the entire issue. We don't have priorities for proper parts of issues. I guess what you meant is that the presence of that particular item merits increasing the priority of the entire issue above "minor," which is fine.

unman commented on Apr 16, 2019 Member

@brendanhoar Other than the Xfce specific issue, do you think any of the others rank above minor?
As I said, KDE doesn't store anything like that information, so provides a solution to that issue. I wonder if it would be worth highlighting this in the docs - in the Privacy section? As a FAQ item?

brendanhoar commented on Apr 16, 2019 • edited ▾ Author

@unman

1. The xfwm4 state file disposable VM content leakage issue is non-minor, yes. I would consider it major actually.
2. Old snapshot/volatile volumes from disposable VMs (perhaps not properly shut down) sitting around forever, I would also consider major.
3. The rest of the items are perhaps lower, but I have not performed triage.

However, I posit that the forensic value of knowing each and every disposable VM invocation from the date of installation (e.g. October 2018 on the installation I tested) may bump some of the other items out of the minor status even if they do not contain contents of disposable VM sessions.

Perhaps I should break these out into separate issues grouped in some way?

In my first post on this issue, I asked the qubes developers team to perform triage, but perhaps that is on me as the reporting user?

At first glance, a good portion of the reported items related to logs/dmesg/console outputs could be mitigated either by via reduction of logging or by date-limited log rotation w/ scrub/ erasure of files > n days old...or both.

Thanks,
Brendan

> *Perhaps I should break these out into separate issues grouped in some way?*
>
> In my first post on this issue, I asked the qubes developers team to perform triage, but perhaps that is on me as the reporting user?

There are two kinds of triage:

1. Issue tracking: categorizing and labeling issues, ensuring that they're not duplicates, etc.
2. Determining importance to the project: how the issue affects security and user experience, whether it's on our development roadmap, etc.

It sounds like you're thinking of the second one. Ultimately, we (not you) are responsible for both of these, but issue reporters can always help us with these by following the issue reporting guidelines -- in particular, filing separate issues separately.

brendanhoar commented on Apr 17, 2019 Author

@andrewdavidwong - Thanks for the very clear response!

Would you recommend that I spin-off a new separate issue for dispVM "content" remaining on the dom0 filesystem (I feel these are less likely to be considered "minor") and leave only the dispVM "usage history" items here? I would also modify the original post to note what was split out so as to not confuse people reading the issue thread later.

B

andrewdavidwong commented on Apr 18, 2019 Member

> **@andrewdavidwong** - Thanks for the very clear response!
>
> Would you recommend that I spin-off a new separate issue for dispVM "content" remaining on the dom0 filesystem (I feel these are less likely to be considered "minor") and leave only the dispVM "usage history" items here? I would also modify the original post to note what was split out so as to not confuse people reading the issue thread later.
>
> B

Sure, that sounds good. Thanks!

marmarek mentioned this issue on Apr 18, 2019

Improve auto_cleanup mechanism #4984

Open

Qubes Domains: "Open File Manager" button similar to "Run Terminal" #5170

Closed

brendanhoar mentioned this issue on May 13, 2020

Add additional qubes logs to logrotate #5820

Closed

unman mentioned this issue on Nov 22, 2020

DisposableVM logs not discarded in /var/log/qubes/guid.[dispxxx].log #6222

Closed

marmarek mentioned this issue on Feb 4, 2021

Don't log to qubes.log or vm-*.log files on disk, only stderr QubesOS/qubes-core-admin#386

Merged

zithro commented on Feb 28, 2022

Data logged to `/var/log/xen/console/hypervisor.log` -may- also be found in `xl dmesg`, but :

- by default Qubes (Xen ?) doesn't log guest info in there (Guest Loglevel: Nothing [...]), but it may good to add it to the list for people debugging by altering Xen command line (guest_loglvl=LVL) then FORGET to remove/reset to default.
- the xl dmesg ring buffer is only 16k and is cleared on shutdown, but not hypervisor.log.

I know this is an edge case, but I think that more warnings are better than none.
Little trick, one can fill up the live ring buffer to remove sensitive information by running `xl debug-keys X` and using the more verbose command a few times. Ofc it would need to delete information afterwards from `hypervisor.log` too.

mati7337 commented on Nov 24, 2022

QubesOS/qubes-desktop-linux-xfce4#28 should take care of the xfwm4-*.state files

andrewdavidwong removed this from the **Release TBD** milestone on Aug 13, 2023

`Keep state files only when SaveOnExit is true` … 1c087f8

Assignees

No one assigned

Labels

C: other help wanted P: default privacy T: enhancement

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

8 participants