New issue

Jump to bottom

The default permissions used by atomic_move can create files that are world readable #67794

Closed samdoran opened this issue on Feb 26, 2020 · 20 comments · Fixed by #68970 or #70221

Labels affects_2.10 bug has_pr security support:core

samdoran commented on Feb 26, 2020 • edited Contributor

SUMMARY

CVE-2020-1736

If a file doesn't exist, we create it with `0666` permissions combined with the current `umask`. Depending on the default umask as well as the permissions on the destination directory, this could result in world readable files.

Relevant code:
Default permissions:

ansible/lib/ansible/module_utils/common/file.py
Lines 60 to 62 in 79dfae9

```
60      _PERM_BITS = 0o7777          # file mode permission bits
61      _EXEC_PERM_BITS = 0o0111     # execute permission bits
62      _DEFAULT_PERM = 0o0666       # default file permission bits
```

creation in `atomic_move`:

ansible/lib/ansible/module_utils/basic.py
Lines 2296 to 2303 in 79dfae9

```
2296      if creating:
2297          # make sure the file has the correct permissions
2298          # based on the current value of umask
2299          umask = os.umask(0)
2300          os.umask(umask)
2301          os.chmod(b_dest, DEFAULT_PERM & ~umask)
2302          try:
2303              os.chown(b_dest, os.geteuid(), os.getegid())
```

```
if creating:
    # make sure the file has the correct permissions
    # based on the current value of umask
    umask = os.umask(0)
    os.umask(umask)
    os.chmod(b_dest, DEFAULT_PERM & ~umask)
    try:
        os.chown(b_dest, os.geteuid(), os.getegid())
    except OSError:
        # We're okay with trying our best here.  If the user is not
        # root (or old Unices) they won't be able to chown.
        pass
```

Suggested correction is to use more restrictive permissions by default and/or add a mechanism to prevent creating world readable files.

ISSUE TYPE

- Bug Report

COMPONENT NAME

```
ansible/lib/ansible/module_utils/common/file.py
ansible/lib/ansible/module_utils/basic.py
```

ANSIBLE VERSION

```
2.10
```

CONFIGURATION

```
default
```

OS / ENVIRONMENT

STEPS TO REPRODUCE

EXPECTED RESULTS

ACTUAL RESULTS

samdoran added the security label on Feb 26, 2020

ansibot commented on Feb 26, 2020 — Contributor

Files identified in the description:
None

If these files are inaccurate, please update the `component name` section of the description or use the `!component` bot command.

click here for bot help

ansibot added affects_2.10 bug support:core labels on Feb 26, 2020

ansibot commented on Feb 26, 2020 — Contributor

Files identified in the description:

- `lib/ansible/module_utils/basic.py`
- `lib/ansible/module_utils/common/file.py`

If these files are inaccurate, please update the `component name` section of the description or use the `!component` bot command.

click here for bot help

bcoca commented on Apr 2, 2020 — Member

ansible/ansible-stage#34

ansibot added the has_pr label on Apr 2, 2020

bcoca self-assigned this on Apr 3, 2020

bcoca added a commit to bcoca/ansible that referenced this issue on Apr 15, 2020

`stricter permissions on atomic_move when creating new file` ··· `1205650`

bcoca mentioned this issue on Apr 15, 2020

stricter permissions on atomic_move when creating new file #68970

Merged

bcoca added a commit to bcoca/ansible that referenced this issue on Apr 15, 2020

`stricter permissions on atomic_move when creating new file` ··· `a2ef19e`

bcoca closed this as completed in #68970 on Apr 16, 2020

---

bcoca added a commit that referenced this issue on Apr 16, 2020

`stricter permissions on atomic_move when creating new file (#68970)` ··· `566f246`

bcoca added a commit to bcoca/ansible that referenced this issue on Apr 16, 2020

`stricter permissions on atomic_move when creating new file (ansible#6…` ··· `2127777`

bcoca added a commit to bcoca/ansible that referenced this issue on Apr 16, 2020

`stricter permissions on atomic_move when creating new file (ansible#6…` ··· `43fa2d1`

This was referenced on Apr 16, 2020

stricter permissions on atomic_move when creating new file (#68970) #68976

Closed

stricter permissions on atomic_move when creating new file (#68970) #68977

Closed

bcoca reopened this on Apr 16, 2020

bcoca commented on Apr 16, 2020 — Member

reopened since PR that had been merged was reverted due to much larger impact than initially forseen.

mweinelt mentioned this issue on May 5, 2020

ansible: v2.9.2 → v2.9.7, v2.8.7 → v2.8.11, v2.7.15 → v2.7.17 NixOS/nixpkgs#86980

Merged

10 tasks

brianmay commented on May 6, 2020

@bcoca Can you please point me to the commit were this was reverted? I am not seeing it.
https://github.com/bcoca/ansible/commits/2127777856f81bd03666db5a68b379901a849845/lib/ansible/module_utils/common/file.py

bcoca commented on May 6, 2020 Member

`5733660`

brianmay commented on May 7, 2020

OK, so according to #68983 it appears this was reverted because we broke some tests in collections. What is the solution? Maybe we need a `DEFAULT_UMASK` setting or something. initially this could be 666, over time we could work to move this to 660.

ansibot added the needs_triage label on May 17, 2020

jimi-c removed the needs_triage label on May 19, 2020

jimi-c mentioned this issue on May 29, 2020

copy module creates destination file initially with umask of connection context rather than secure or specified mode #46971

Closed

samdoran assigned **samdoran** and unassigned **bcoca** on Jun 18, 2020

samdoran mentioned this issue on Jun 22, 2020

Change default file permissions so they are not world readable #70221

Merged

3 tasks

31 hidden items
Load more...

nre-ableton added a commit to Ableton/ansible-role-jenkins-jcasc that referenced this issue on Aug 18, 2020

`Add modes for file-related modules` ··· `b61985b`

yaobinwen-mvs mentioned this issue on Aug 18, 2020

Missing 'mode' on file copy can lead to too restrictive default permissions geerlingguy/ansible-for-devops#314

Closed

eoli3n commented on Aug 19, 2020 • edited Contributor

It broke my playbook too.

> Ansible should do the expected thing of deferring to the system umask or mode in the module for permissions on the final file.

Yes it should.

👍 4

ghost pushed a commit to Ableton/ansible-role-jenkins-jcasc that referenced this issue on Aug 19, 2020

`Add modes for file-related modules` ··· `94913a2`

nre-ableton added a commit to Ableton/ansible-role-jenkins-jcasc that referenced this issue on Aug 19, 2020

`Add modes for file-related modules` ··· `a692471`

HontoNoRoger commented on Aug 20, 2020

I also ran into this issue today, using Ansible 2.9.12 from the Launchpad Ansible repo:
`http://ppa.launchpad.net/ansible/ansible/ubuntu bionic/main amd64 Packages`

Could it be that is hasn't been reverted there? It is causing a lot of trouble for our automated installations currently.

relrod commented on Aug 20, 2020 Member

Correct, there has not yet been another release since the change was reverted. The revert will be in the next 2.9 release.

n-cc commented on Aug 20, 2020

Is there a timeline for a new release? I'm specifically interested in 2.8, but it'd probably be helpful to know both.

relrod commented on Aug 20, 2020 — Member

Likely around 8/31 or 9/1. Releases typically happen every 3 weeks (though that is changing slightly, soon).

TuxInvader mentioned this issue on Aug 21, 2020

Set file permissions on APT configuration files and keys nginxinc/ansible-role-nginx#308

Closed

openstack-mirroring pushed a commit to openstack/openstack-ansible-os_tempest that referenced this issue on Aug 22, 2020

`Set mode for copy operation` ··· `3e590ab`

openstack-mirroring pushed a commit to openstack/openstack that referenced this issue on Aug 22, 2020

`Update git submodules` ··· `dbcc605`

netbsd-srcmastr pushed a commit to NetBSD/pkgsrc that referenced this issue on Aug 24, 2020

`ansible: updated to 2.9.12` ··· `5f51bb6`

mamedin mentioned this issue on Aug 28, 2020

CentOS deploy with ansible >=2.9.12 fails (permissions issue) archivematica/Issues#1297

Open

5 tasks

OldCrowEW mentioned this issue on Aug 28, 2020

correct linting 208 issues OldCrowEW/ansible-role-hashicorp-consul#16

Merged

jahsome mentioned this issue on Sep 1, 2020

File '...REVISION' created with default permissions '600' warning ansistrano/deploy#361

Closed

samy-mahmoudi added a commit to samy-mahmoudi/ansible that referenced this issue on Oct 6, 2020

`docs: Mention CVE-2020-1736 in the copy module` ··· `4692663`

samy-mahmoudi mentioned this issue on Oct 6, 2020

docs: Mention CVE-2020-1736 in the documentation #72127

Closed

samy-mahmoudi added a commit to samy-mahmoudi/ansible that referenced this issue on Oct 6, 2020

`docs: Mention CVE-2020-1736 in the copy module` ··· `c78839d`

samy-mahmoudi added a commit to samy-mahmoudi/ansible that referenced this issue on Oct 7, 2020

`docs: Mention CVE-2020-1736 as a comment of 'mode'` ··· `4eb9b72`

ansibot commented on Feb 16, 2021 — Contributor

Files identified in the description:

- `docs/docsite/_extensions/pygments_lexer.py`
- `lib/ansible/module_utils/basic.py`
- `lib/ansible/module_utils/common/file.py`

If these files are incorrect, please update the `component name` section of the description or use the `!component` bot command.

click here for bot help

ansibot commented on Feb 24, 2021 — Contributor

Files identified in the description:

- `lib/ansible/module_utils/basic.py`
- `lib/ansible/module_utils/common/file.py`

If these files are incorrect, please update the `component name` section of the description or use the `!component` bot command.

click here for bot help

samdoran removed their assignment on Jul 13, 2021

mvorisek commented on Dec 7, 2021

I wonder is there any Ansible config where I can simply set the default file/dir mode or umask to 0644? Or is 0644 always the default?

leegarrett commented on Dec 7, 2021 Contributor

> I wonder is there any Ansible config where I can simply set the default file/dir mode or umask to 0644? Or is 0644 always the default?

Read the bug report. The current umask is whatever the target system has set as default, which for Debian-based systems is 0022. You **don't** want to set it to 0644. IMHO this isn't a security bug, because you have to deliberately set the umask to make files world-readable ... to get world-readable files.

mvorisek commented on Dec 7, 2021

I meant if the 0022 umask can be enforced as a default by ansible configuration.

leegarrett commented on Dec 7, 2021 Contributor

> I meant if the 0022 umask can be enforced as a default by ansible configuration.

Please ask in a support channel as this is unrelated to the bug report.

bcoca commented on Jul 20 Member

closing this as it is not really an ansible bug, but how the user has configured umask on their system.

bcoca closed this as completed on Jul 20

ansible locked and limited conversation to collaborators on Jul 27

Assignees

No one assigned

Labels

affects_2.10 **bug** has_pr security **support:core**

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

stricter permissions on atomic_move when creating new file
bcoca/ansible

Change default file permissions so they are not world readable
samdoran/ansible

Replace atomic_move() with a higher level function
samdoran/ansible

11 participants