

New issue

Jump to bottom

# Insecure creation of temporary directory for become\_user #67791

Closed samdoran opened this issue on Feb 26, 2020 · 5 comments · Fixed by #68921

Labels affects\_2.10 bug has\_pr security support:core

samdoran commented on Feb 26, 2020

Contributor

## SUMMARY

[CVE-2020-1733](#)

We create a temporary directory for the `become_user` with `umask 077` in `/var/tmp` without first checking if the directory exists and that it has the expected permissions.

## Relevant code

```
ansible/lib/ansible/plugins/shell/__init__.py
Lines 159 to 163 in 79dfae9

159     if mode:
160         tmp_umask = 0o777 & ~mode
161         cmd = '%s umask %o %s %s %s' % (self._SHELL_GROUP_LEFT, tmp_umask, self._SHELL_AND, cmd, self._SHELL_GROUP_RIGHT)
162
163     return cmd
```

We need to validate the parent directories are as expected before creating directories in those paths and fail if the permissions and/or ACLs are not what we expect.

## ISSUE TYPE

- Bug Report

## COMPONENT NAME

`lib/ansible/plugins/shell/__init__.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:

- `lib/ansible/plugins/action/shell.py`
- `lib/ansible/plugins/shell/__init__.py`
- `lib/ansible/plugins/shell/cmd.py`
- `lib/ansible/plugins/shell/csh.py`
- `lib/ansible/plugins/shell/fish.py`
- `lib/ansible/plugins/shell/powershell.py`
- `lib/ansible/plugins/shell/sh.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](#)

ansibot commented on Feb 26, 2020

Contributor

cc @jborean93 @nitzmahone  
[click here for bot help](#)

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

**ansibot** commented on Mar 29, 2020

Contributor

Files identified in the description:

- `lib/ansible/plugins/action/shell.py`
- `lib/ansible/plugins/shell/__init__.py`
- `lib/ansible/plugins/shell/cmd.py`
- `lib/ansible/plugins/shell/powershell.py`
- `lib/ansible/plugins/shell/sh.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](#)


 **sshedi** mentioned this issue on Apr 4, 2020

**ensure secure creation of tmpdir for become\_user** #68692

 Closed

**sshedi** commented on Apr 4, 2020

@samdoran Please review this change, this is my first PR, please pardon me if you find any mistakes.

 **ansibot** added the `has_pr` label on Apr 4, 2020

**bcoca** commented on Apr 6, 2020


Member

I would say we need to check 'after' since any check 'before' would be subject to race conditions

 **bcoca** added a commit to `bcoca/ansible` that referenced this issue on Apr 13, 2020

 `avoid mkdir -p ...`


9b9c137

 **bcoca** mentioned this issue on Apr 13, 2020

**avoid mkdir -p** #68921

 Merged

 **bcoca** closed this as completed in [#68921](#) on Apr 13, 2020

 **bcoca** added a commit that referenced this issue on Apr 13, 2020

 `avoid mkdir -p (#68921) ...`

8b77d8e

 **bcoca** added a commit to `bcoca/ansible` that referenced this issue on Apr 13, 2020

 `avoid mkdir -p (ansible#68921) ...`

c79e12b

 **bcoca** added a commit to `bcoca/ansible` that referenced this issue on Apr 13, 2020

 `avoid mkdir -p (ansible#68921) ...`

0331931

 **bcoca** added a commit to `bcoca/ansible` that referenced this issue on Apr 13, 2020

 `avoid mkdir -p (ansible#68921) ...`

0a85e91

 This was referenced on Apr 13, 2020

**avoid mkdir -p ([#68921](#))** #68926

 Merged

**avoid mkdir -p ([#68921](#))** #68927

 Merged


**avoid mkdir -p ([#68921](#))** #68928

 Merged

 **mattclay** pushed a commit that referenced this issue on Apr 14, 2020


 `avoid mkdir -p (#68921) ...`

80b9a0a

 **mattclay** pushed a commit that referenced this issue on Apr 14, 2020


 avoid mkdir -p (#68921) (#68927) ...

8251d9f

 mattclay pushed a commit that referenced this issue on Apr 14, 2020

 avoid mkdir -p (#68921) (#68928) ...

ecf99d5

 ansible locked and limited conversation to collaborators on May 11, 2020

#### 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.

 avoid mkdir -p  
boca/ansible

 ensure secure creation of tmpdir for become\_user

#### 4 participants

