

New issue

Jump to bottom

fetch module path traversal #67793

Closed samdoran opened this issue on Feb 26, 2020 · 2 comments · Fixed by #68720

Assignees



Labels

affects_2.10 bug files has_pr module security support:core

samdoran commented on Feb 26, 2020

Contributor

SUMMARY

[CVE-2020-1735](#)

Possibly related to [CVE-2019-3828](#) (#52133)

The `fetch` module takes the `source` result from the `slurp` module, which came from the remote host. We don't really validate this path and it could have been manipulated by the remote host in a malicious way such that we end up a path similar to `/tmp/result_fetch/ansible1/../../../../../../../../../../../../home/<user>/.profile` for the source. This allows an attacker to place a file the contents of which they control.

Relevant Code:

ansible/lib/ansible/plugins/action/fetch.py
Lines 83 to 102 in 79dfae9

```
83 slurpres = self._execute_module(module_name='slurp', module_args=dict(src=source), task_vars=task_vars)
84 if slurpres.get('failed'):
85     if not fail_on_missing and (slurpres.get('msg').startswith('file not found') or remote_checksum == '1'):
86         result['msg'] = "the remote file does not exist, not transferring, ignored"
87         result['file'] = source
88         result['changed'] = False
89     else:
90         result.update(slurpres)
91     return result
92 else:
93     if slurpres['encoding'] == 'base64':
94         remote_data = base64.b64decode(slurpres['content'])
```

Suggested correction from the reporter:

- Don't use `%s/%s/%s` to compute the destination file or clean the last argument
- add the following check:

```
target_dir = os.path.normpath(os.path.join(self._loader.path_dwim(dest), target_name))
dest = os.path.normpath(os.path.join(target_dir, source_local))
assert os.path.commonpath([target_dir, dest]) == target_dir
```

ISSUE TYPE

- Bug Report

COMPONENT NAME

lib/ansible/plugins/action/fetch.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




 **samdoran** changed the title ~~Fetch module path traversal~~ fetch module path traversal on Feb 26, 2020

 **samdoran** self-assigned this on Feb 26, 2020

samdoran commented on Feb 26, 2020

Contributor Author

`os.path.commonpath()` was added in Python 3.4 but is not available in Python 2.7, so we cannot use that. `os.path.commonprefix()` is available in Python 2.7 and should work, though.

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

 **samdoran** mentioned this issue on Feb 26, 2020


fetch - normalize and validate paths #67801

Closed

bcoca commented on Apr 1, 2020

Member

we can just remove those lines since we already do remote-expand previously, there is no need to use the return from slurp.

 **ansibot** added the `has_pr` label on Apr 1, 2020

 **bcoca** assigned **bcoca** and unassigned **samdoran** on Apr 3, 2020

 **bcoca** added a commit to `bcoca/ansible` that referenced this issue on Apr 6, 2020

fixed fetch traversal from slurp ...


bddbaa6

 **bcoca** mentioned this issue on Apr 6, 2020

fixed fetch traversal from slurp #68720

Merged

 **bcoca** closed this as completed in [#68720](#) on Apr 8, 2020

 **bcoca** added a commit that referenced this issue on Apr 8, 2020

fixed fetch traversal from slurp ([#68720](#)) ...

ba87c22

 **bcoca** added a commit to `bcoca/ansible` that referenced this issue on Apr 8, 2020

fixed fetch traversal from slurp ([ansible#68720](#)) ...

5292482

 **bcoca** added a commit to `bcoca/ansible` that referenced this issue on Apr 8, 2020

fixed fetch traversal from slurp ([ansible#68720](#)) ...

ea82e7

 **bcoca** mentioned this issue on Apr 8, 2020

fixed fetch traversal from slurp (#68720) #68780

Merged

 **bcoca** added a commit to `bcoca/ansible` that referenced this issue on Apr 8, 2020

fixed fetch traversal from slurp ([ansible#68720](#)) ...

0a5f588

 This was referenced on Apr 8, 2020

fixed fetch traversal from slurp (#68720) #68781

Merged

fixed fetch traversal from slurp (#68720) #68782

Merged

 **bcoca** added a commit to `bcoca/ansible` that referenced this issue on Apr 9, 2020


fixed fetch traversal from slurp ([ansible#68720](#)) ...

f45cb36

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































fixed fetch traversal from slurp ([ansible#68720](#)) ...

6c3d086

 **mattclay** pushed a commit that referenced this issue on Apr 15, 2020

fixed fetch traversal from slurp ([#68720](#)) ...

290bfa8

-  **mattclay** pushed a commit that referenced this issue on Apr 15, 2020
-  Fixed fetch traversal from slurp (#68720) ...
- 6f75aa2
-  **mattclay** pushed a commit that referenced this issue on Apr 15, 2020
-  Fixed fetch traversal from slurp (#68720) ...
- 3c48483
-  **relirod** added a commit to relirod/ansible that referenced this issue on Apr 18, 2020
-  Fix incorrect CVE reference in changelog fragment ...
- b4d0269
-  **relirod** added a commit to relirod/ansible that referenced this issue on Apr 18, 2020
-  Fix incorrect CVE reference in changelog fragment ...
- 7bc2c16
-  **relirod** added a commit to relirod/ansible that referenced this issue on Apr 18, 2020
-  Fix incorrect CVE reference in changelog fragment ...
- 3c33975
-  **relirod** added a commit to relirod/ansible that referenced this issue on Apr 18, 2020
-  Fix incorrect CVE reference in changelog fragment ...
- d90a197
-  This was referenced on Apr 18, 2020
- Fix incorrect CVE reference in changelog fragment (devel) #69022**
-  Merged
- Fix incorrect CVE reference in changelog fragment (2.9) #69023**
-  Merged
- Fix incorrect CVE reference in changelog fragment (2.8) #69024**
-  Merged
- Fix incorrect CVE reference in changelog fragment (2.7) #69025**
-  Merged
-  **mattclay** pushed a commit that referenced this issue on Apr 21, 2020
-  Fix incorrect CVE reference in changelog fragment ...
- ✖ 2a90e9b
-  **mattclay** pushed a commit that referenced this issue on Apr 21, 2020
-  Fix incorrect CVE reference in changelog fragment ...
- ✖ 18f91bb
-  **mattclay** pushed a commit that referenced this issue on Apr 21, 2020
-  Fix incorrect CVE reference in changelog fragment ...
- ✖ 40969ff
-  **mattclay** pushed a commit that referenced this issue on Apr 21, 2020
-  Fix incorrect CVE reference in changelog fragment ...
- ✖ de9a4f5
-  **bcoca** pushed a commit to bcoca/ansible that referenced this issue on Apr 22, 2020
-  Fix incorrect CVE reference in changelog fragment ...
- b0af011
-  **bcoca** pushed a commit to bcoca/ansible that referenced this issue on Apr 28, 2020
-  Fix incorrect CVE reference in changelog fragment ...
- f7ad072
-  **ansible** locked and limited conversation to collaborators on May 6, 2020

Assignees

 bcoca

Labels

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

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 fixed fetch traversal from slurp

bcoca/ansible
❗❗ fetch - normalize and validate paths
samdoran/ansible

3 participants

