Bug 917904 (CVE-2013-1815) - CVE-2013-1815 OpenStack packstack: answerfile creation permissions issue

Keywords: Security

Status: CLOSED ERRATA

Alias: CVE-2013-1815

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: ~~Red Hat Product Security~~

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 917905

Blocks: 917906

TreeView+ depends on / blocked

Reported: 2013-03-05 05:03 UTC by ~~Kurt Seifried~~

Modified: 2023-05-12 17:30 UTC (History)

CC List: 10 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed: 2013-04-08 17:53:35 UTC

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2013:0671	0	normal	SHIPPED_LIVE	Moderate: openstack-packstack security and bug fix update	2013-03-21 22:22:21 UTC

~~Kurt Seifried~~ 2013-03-05 05:03:59 UTC Description

```
Derek Higgins (derekh) of Red Hat reports:
```

packstack creates a answerfile containing configuration details for an
openstack deployment. But after a recent comment in ~~https://bugzilla.redhat.com/show_bug.cgi?id=906410~~ [Open URL] comment 4, I
reviewed the code on how it is generated.

The file was being opened, written to and then the mode was being changed to
600:

https://github.com/stackforge/packstack/blob/07a7897038bee143630fd84e95b3a4f5c89a5b47/packstack/installer/run_setup.py

```
def generateAnswerFile(outputFile, overrides={}):
    sep = os.linesep
    fmt = ("%(comment)s%(separator)s%(conf_name)s=%
(default_value)s"
           "%(separator)s")
    outputFile = os.path.expanduser(outputFile)
    with open(outputFile, "w") as ans_file:
...
    os.chmod(outputFile, 0600)
```

and the answer path is provided by:

```
def _getanswerfilepath():
    path = None
    msg = "Could not find a suitable path on which to create
the answerfile"

    # We'll use the first path with
    # write permissions. Order matters.
    for p in ["./", "~/", "/tmp"]:
        if os.access(p, os.W_OK):
            path = os.path.abspath(
```

The current directory "./" may be accessible to an attacker, and "/tmp" is
definitely accessible to attackers. The file permissions should also be set
securely prior to placing the information in it.

Derek Higgins 2013-03-05 09:24:54 UTC Comment 2

Fix merged upstream
https://review.openstack.org/#/c/22986/

~~Murray McAllister~~ 2013-03-19 04:50:43 UTC Comment 3

Acknowledgements:

This issue was discovered by Derek Higgins of the Red Hat

OpenStack team.

errata-xmlrpc 2013-03-21 18:24:25 UTC Comment 4

This issue has been addressed in following products:

  OpenStack Folsom for RHEL 6

Via RHSA-2013:0671 https://rhn.redhat.com/errata/RHSA-2013-0671.html

Note

You need to log in before you can comment on or make changes to this bug.