# Bug 908101 (CVE-2013-0261) - CVE-2013-0261 OpenStack packstack: insecure use of /tmp in manifest creation

**Keywords:** Security

**Status:** CLOSED ERRATA

**Alias:** CVE-2013-0261

**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:** 908102 908103

**Blocks:**

**TreeView+** depends on / blocked

**Reported:** 2013-02-05 21:41 UTC by ~~Kurt Seifried~~

**Modified:** 2023-05-12 17:22 UTC (History)

**CC List:** 9 users (show)

**Fixed In Version:**

**Clone Of:**

**Environment:**

**Last Closed:** 2013-08-09 04:31:14 UTC

**Embargoed:**

| Attachments | (Terms of Use) |
|---|---|

**Links**

| System | ID | Private | Priority | Status | Summary | Last Updated |
|---|---|---|---|---|---|---|
| Red Hat Product Errata | RHSA-2013:0595 | 0 | normal | SHIPPED_LIVE | Moderate: openstack-packstack security and bug fix update | 2013-03-06 02:00:00 UTC |

~~Kurt Seifried~~ 2013-02-05 21:41:30 UTC Description

```
Kurt Seifried of Red Hat reports:

./packstack/installer/basedefs.py
```

```
============
VAR_DIR = os.path.join("/var/tmp/packstack",
datetime.datetime.now().strftime('%Y%m%d-%H%M'))
DIR_LOG = VAR_DIR
PUPPET_MANIFEST_DIR = os.path.join(VAR_DIR, "manifests")
============


./packstack/modules/ospluginutils.py
============
def appendManifestFile(manifest_name, data, marker=''):
    if not os.path.exists(basedefs.PUPPET_MANIFEST_DIR):
        os.mkdir(basedefs.PUPPET_MANIFEST_DIR)
    manifestfile = os.path.join(basedefs.PUPPET_MANIFEST_DIR,
manifest_name)
    manifestfiles.addFile(manifestfile, marker)
    with open(manifestfile, 'a') as fp:
        fp.write("\n")
        fp.write(data)
============

So we have several failures here:

1) not setting safe permissions (we don't set permissions/use
os.umask/etc.) which means attackers can read the data,
possibly
modify it/etc.

2) not creating directories safely, there is a potential gap
between
"if not os.path.exists" and the "os.mkdir" amongst other
problems

This can be used to modify manifest files at creation time for
example.
```

~~Murray McAllister~~ 2013-02-22 03:24:17 UTC Comment 3

```
Acknowledgements:

This issue was discovered by Kurt Seifried of the Red Hat
Security Response Team.
```

errata-xmlrpc 2013-03-05 21:03:24 UTC Comment 4

```
This issue has been addressed in following products:

  OpenStack Folsom for RHEL 6

Via RHSA-2013:0595 https://rhn.redhat.com/errata/RHSA-2013-
0595.html
```

Note

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