



Bug 909012 (CVE-2013-0270) - CVE-2013-0270 OpenStack Keystone: Large HTTP request DoS

Keywords: Security ✕

Reported: 2013-02-08 03:32 UTC by Kurt Seifried

Status: CLOSED ERRATA

Modified: 2023-05-13 00:08 UTC [\(History\)](#)

Alias: CVE-2013-0270

CC List: 8 users ([show](#))

Product: Security Response

Fixed In Version:

Component: vulnerability

Clone Of:

Version: unspecified

Environment:

Last Closed: 2013-04-04 20:46:55 UTC

Hardware: All

Embargoed:

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 908973 909013

Blocks: 909025

TreeView+ [depends on](#) / [blocked](#)

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

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2013:0708	0	normal	SHIPPED_LIVE	Moderate: openstack-keystone security and bug fix update	2013-04-05 00:19:06 UTC

Kurt Seifried	2013-02-08 03:32:09 UTC	Description
Dan Prince (dprince) reports:		

When long tenant_name is sent few times when requesting token, responsiveness of service decreases until finally it requests ends with MemoryError.

```
keystoneclient.exceptions.AuthorizationFailure: Authorization Failed: Unable to communicate with identity service: Traceback ... MemoryError Includes whole traceback.
```

Memory on keystone host is used up keystone-all process. Also during processing of the request CPU utilization raises for a long time (when and after the first MemoryError state was reached) - like for more than 10 seconds keystone-all can take whole cpu.

Version-Release number of selected component (if applicable):

Name	: openstack-keystone
Arch	: noarch
Version	: 2012.2.1
Release	: 3.el6ost

How reproducible:

Use something similiar to following python example few times (5 times with "len(tenant) == 195000000" for keystone host inside VM with 4GB of RAM)

Actual results:

For first few tries service correctly responds with: (HTTP 400): Authorization Failed: Request attribute tenantName must be less than or equal to 64. The server could not comply with the request because the attribute size is invalid (too large). The client is assumed to be in error.

Later with:

(HTTP 500): Authorization Failed: Unable to communicate with identity service: Traceback (most recent call last):
... whole backtrace here
MemoryError

Most memory of keystone host is used by keystone-all process.

Expected results:

The first 400 error mentioning that attribute is too big for all request (not only first few). And not such a big impact on memory of host.

Additional info:

Similiar to [bug #906178](#) and so also to related upstream bug <https://bugs.launchpad.net/keystone/+bug/1098307> where they mentioned preparation of general check/defense for too big requests.

Kurt Seifried 2013-02-08 04:50:30 UTC

[Comment 2](#)

This is public:
<https://bugs.launchpad.net/keystone/+bug/1099025>

Jan Lieskovsky 2013-02-11 11:20:47 UTC

[Comment 3](#)

Relevant upstream patch against the master branch:
<https://github.com/openstack/keystone/commit/7691276b869a86c2b75631d5bede9f61e030d9d8>

Dan Prince 2013-02-12 18:14:48 UTC

[Comment 4](#)

Kurt: The pipeline change you link above would fix this... but is sort of a new features. I think this commit (already on Folsom stable) is more backportable:

<https://github.com/openstack/keystone/commit/82c87e5638ebaf9f166a9b07a0155291276d6fdc>

Alan Pevec 2013-02-12 18:19:55 UTC

[Comment 5](#)

(In reply to [comment #4](#))
> <https://github.com/openstack/keystone/commit/82c87e5638ebaf9f166a9b07a0155291276d6fdc>
> [82c87e5638ebaf9f166a9b07a0155291276d6fdc](https://github.com/openstack/keystone/commit/82c87e5638ebaf9f166a9b07a0155291276d6fdc)

And this is in openstack-keystone-2012.2.1-3.el6ost just published.

Alan Pevec 2013-03-04 20:16:25 UTC

[Comment 7](#)

(In reply to [comment #3](#))
> Relevant upstream patch against the master branch:
>
> <https://github.com/openstack/keystone/commit/7691276b869a86c2b75631d5bede9f61e030d9d8>
> [7691276b869a86c2b75631d5bede9f61e030d9d8](https://github.com/openstack/keystone/commit/7691276b869a86c2b75631d5bede9f61e030d9d8)

This was proposed for stable/folsom but did not pass review:
<https://review.openstack.org/#/c/22661/>

Murray McAllister 2013-03-27 05:57:23 UTC

[Comment 11](#)

Acknowledgements:

This issue was discovered by Dan Prince of Red Hat.

errata-xmlrpc 2013-04-04 20:22:50 UTC

[Comment 12](#)

This issue has been addressed in following products:

OpenStack Folsom for RHEL 6

Via RHSA-2013:0708 <https://rhn.redhat.com/errata/RHSA-2013-0708.html>

Note

You need to [log in](#) before you can comment on or make changes to this bug.

