

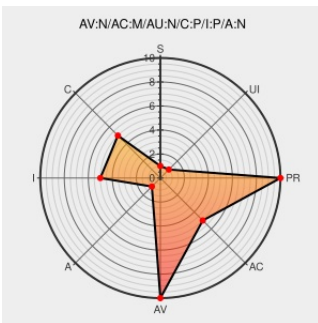


CVE-2013-6396

Published on: 02/18/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:14 AM UTC

CVE-2013-6396

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Swift](#) from [Openstack](#) contain the following vulnerability:

The OpenStack Python client library for Swift (python-swiftclient) 1.0 through 1.9.0 does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.

CVE-2013-6396 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5.8 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Bug #1199783 "Missing SSL cert check in Swift python client (CVE...)" : Bugs : python-swiftclient

[Vendor Advisory](#)
[bugs.launchpad.net](#)
[text/html](#)

[CONFIRM bugs.launchpad.net/python-swiftclient/+bug/1199783](#)

oss-security - [OSSA 2014-005] Missing SSL certificate check in Python Swift client (CVE-2013-6396)

[www.openwall.com](#)
[text/html](#)

[MLIST \[oss-security\] 20140217 \[OSSA 2014-005\] Missing SSL certificate check in Python Swift client \(CVE-2013-6396\)](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Application	Openstack	Swift	1.8.0	rc2	All	All
Application	Openstack	Swift	1.9.0	All	All	All
Application	Openstack	Swift	1.0.0	All	All	All
Application	Openstack	Swift	1.0.1	All	All	All
Application	Openstack	Swift	1.0.2	All	All	All
Application	Openstack	Swift	1.1.0	All	All	All
Application	Openstack	Swift	1.1.0	rc1	All	All
Application	Openstack	Swift	1.1.0	rc2	All	All
Application	Openstack	Swift	1.10.0	All	All	All
Application	Openstack	Swift	1.11.0	All	All	All
Application	Openstack	Swift	1.2.0	All	All	All
Application	Openstack	Swift	1.2.0	gamma1	All	All
Application	Openstack	Swift	1.2.0	rc1	All	All
Application	Openstack	Swift	1.3.0	All	All	All
Application	Openstack	Swift	1.3.0	gamma1	All	All
Application	Openstack	Swift	1.3.0	rc1	All	All
Application	Openstack	Swift	1.4.0	All	All	All
Application	Openstack	Swift	1.4.1	All	All	All
Application	Openstack	Swift	1.4.2	All	All	All
Application	Openstack	Swift	1.4.3	All	All	All
Application	Openstack	Swift	1.4.4	All	All	All
Application	Openstack	Swift	1.4.5	All	All	All
Application	Openstack	Swift	1.4.6	All	All	All
Application	Openstack	Swift	1.4.7	All	All	All
Application	Openstack	Swift	1.4.8	All	All	All
Application	Openstack	Swift	1.5.0	All	All	All
Application	Openstack	Swift	1.6.0	All	All	All
Application	Openstack	Swift	1.7.0	All	All	All
Application	Openstack	Swift	1.7.2	All	All	All
Application	Openstack	Swift	1.7.4	All	All	All
Application	Openstack	Swift	1.7.5	All	All	All
Application	Openstack	Swift	1.7.6	All	All	All
Application	Openstack	Swift	1.8.0	All	All	All
Application	Openstack	Swift	1.8.0	rc1	All	All
Application	Openstack	Swift	1.8.0	rc2	All	All
Application	Openstack	Swift	1.9.0	All	All	All

```
cpe:2.3:a:openstack:swift:1.0.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.1.0:rc1:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.1.0:rc2:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.10.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.11.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.2.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.2.0:gamma1:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.2.0:rc1:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.3.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.3.0:gamma1:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.3.0:rc1:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.4.0:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.4.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.4.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.4.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.4.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.4.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.4.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.4.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.4.8:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.5.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.6.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.7.0:*.~*~*~*~*~*~*~*~*~*
```

```
cpe:2.3:a:openstack:swift:1.7.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:openstack:swift:1.7.4:*:*:*:*:*:*:
```

cpe:2.3:a:openstack:swift:1.7.5:~::~::~:
cpe:2.3:a:openstack:swift:1.7.6:~::~::~:
cpe:2.3:a:openstack:swift:1.8.0:~::~::~:
cpe:2.3:a:openstack:swift:1.8.0:rc1:~::~::~:
cpe:2.3:a:openstack:swift:1.8.0:rc2:~::~::~:
cpe:2.3:a:openstack:swift:1.9.0:~::~::~:
cpe:2.3:a:openstack:swift:1.0.0:~::~::~:
cpe:2.3:a:openstack:swift:1.0.1:~::~::~:
cpe:2.3:a:openstack:swift:1.0.2:~::~::~:
cpe:2.3:a:openstack:swift:1.1.0:~::~::~:
cpe:2.3:a:openstack:swift:1.1.0:rc1:~::~::~:
cpe:2.3:a:openstack:swift:1.1.0:rc2:~::~::~:
cpe:2.3:a:openstack:swift:1.10.0:~::~::~:
cpe:2.3:a:openstack:swift:1.11.0:~::~::~:
cpe:2.3:a:openstack:swift:1.2.0:~::~::~:
cpe:2.3:a:openstack:swift:1.2.0:gamma1:~::~::~:
cpe:2.3:a:openstack:swift:1.2.0:rc1:~::~::~:
cpe:2.3:a:openstack:swift:1.3.0:~::~::~:
cpe:2.3:a:openstack:swift:1.3.0:gamma1:~::~::~:
cpe:2.3:a:openstack:swift:1.3.0:rc1:~::~::~:
cpe:2.3:a:openstack:swift:1.4.0:~::~::~:
cpe:2.3:a:openstack:swift:1.4.1:~::~::~:
cpe:2.3:a:openstack:swift:1.4.2:~::~::~:
cpe:2.3:a:openstack:swift:1.4.3:~::~::~:
cpe:2.3:a:openstack:swift:1.4.4:~::~::~:
cpe:2.3:a:openstack:swift:1.4.5:~::~::~:
cpe:2.3:a:openstack:swift:1.4.6:~::~::~:
cpe:2.3:a:openstack:swift:1.4.7:~::~::~:
cpe:2.3:a:openstack:swift:1.4.8:~::~::~:

cpe:2.3:a:openstack:swift:1.5.0:*****:
cpe:2.3:a:openstack:swift:1.6.0:*****:
cpe:2.3:a:openstack:swift:1.7.0:*****:
cpe:2.3:a:openstack:swift:1.7.2:*****:
cpe:2.3:a:openstack:swift:1.7.4:*****:
cpe:2.3:a:openstack:swift:1.7.5:*****:
cpe:2.3:a:openstack:swift:1.7.6:*****:
cpe:2.3:a:openstack:swift:1.8.0:*****:
cpe:2.3:a:openstack:swift:1.8.0:rc1:*****:
cpe:2.3:a:openstack:swift:1.8.0:rc2:*****:
cpe:2.3:a:openstack:swift:1.9.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)