# CVE Detail – CVE-2012-4406

OpenStack Object Storage (swift) before 1.7.0 uses the loads function in the pickle Python module unsafely when storing and loading metadata in memcached, which allows remote attackers to execute arbitrary code via a crafted pickle object.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.91536

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-502: Deserialization of Untrusted Data

## CAPEC(s)

* CAPEC-586: Object Injection

## Affected Products

* cpe:2.3:a:openstack:swift:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:16:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:redhat:gluster\_storage\_management\_console:2.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:redhat:gluster\_storage\_server\_for\_on-premise:2.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:redhat:storage:2.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:redhat:storage\_for\_public\_cloud:2.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:6.0:\*:\*:\*:\*:\*:\*:\*