CVE-2012-4456

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2012-4456
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-10-09 15:55:00 UTC
Updated	2023-02-13 04:34:00 UTC
Description	The (1) OS-KSADM/services and (2) tenant APIs in OpenStack Keystone Essex before 2012.1.2 and Folsom before folsom

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openstack	Keystone	All	All	All	All
Application	Openstack	Keystone	2012.2	milestone1	All	All
Application	Openstack	Keystone	All	All	All	All
Application	Openstack	Keystone	2012.2	milestone1	All	All

References

Reference
Bug #1006822 “[OSSA 2012-015] API v2.0/OS-KSADM/services, v2.0/O...” : Bugs : Keystone
Require authz for user role list (bug 1006815) · openstack/keystone@14b136a · GitHub
861179 – (CVE-2012-4456) CVE-2012-4456 Openstack Keystone 2012.1.1: fails to validate tokens in Admin API
OpenStack Keystone Token Validation Multiple Security Bypass Vulnerabilities
IBM X-Force Exchange
oss-security - [OSSA 2012-015] Some actions in Keystone admin API do not validate token (CVE-2012-4456)
[OSSA 2012-015] Some actions in Keystone admin API do not validate token (CVE-2012-4456) : Mailing list archive : openstack team in Laun
Require authz for user role list (bug 1006815) · openstack/keystone@8680549 · GitHub
Bug #1006815 “[OSSA 2012-015] Admin API /v2.0/tenants/{tenant_id...” : Bugs : Keystone
Red Hat Customer Portal

Security Alerts - Secunia
CVE-2012-4456 - Red Hat Customer Portal
Require authz for service CRUD (bug 1006822) · openstack/keystone@24df3ad · GitHub
Require authz for service CRUD (bug 1006822) · openstack/keystone@1d146f5 · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**