



CVE-2012-4457

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

Summary

CVE	CVE-2012-4457
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-10-09 15:55:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	OpenStack Keystone Essex before 2012.1.2 and Folsom before folsom-3 does not properly handle authorization tokens for

Risk And Classification

Primary CVSS: v2.0 4 from nvd@nist.gov

AV:N/AC:L/Au:S/C:P/I:N/A:N

Problem Types: CWE-287 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:S/C:P/I:N/A:N

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	2012.2	milestone2	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version		Platforms	
CNA	Na	N/a	affected n/a		Not specified	
References						
Reference						
Security Alerts - Secunia						
Raise unauthorized if tenant disabled (bug 988920) · openstack/keystone@5373601 · GitHub						
[OSSA 2012-016] Token authorization for a user in a disabled tenant is allowed (CVE-2012-4457) : Mailing list archive : openstack team in La						
IBM X-Force Exchange						
OpenStack Keystone Token Validation Multiple Security Bypass Vulnerabilities						
861180 – (CVE-2012-4457) CVE-2012-4457 OpenStack Keystone 2012.1.1: fails to raise Unauthorized user error for disabled tenant						
Raise unauthorized if tenant disabled (bug 988920) · openstack/keystone@4ebfdfa · GitHub						
oss-security - [OSSA 2012-016] Token authorization for a user in a disabled tenant is allowed (CVE-2012-4457)						
CVE Program record						
NVD vulnerability detail						
No vendor comments have been submitted for this CVE.						
Legacy QID Mappings						
996740 Python (Pip) Security Update for Keystone (GHSA-x8h4-xf47-pqc3)						