Openstack keystone: openstack keystone: authorization bypass via improper ec2 token handling

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

Summary

CVE	CVE-2012-5571
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-12-18 01:55:03 UTC
Updated	2026-04-07 07:16:22 UTC
Description	A flaw was found in OpenStack Keystone. This vulnerability allows remote authenticated users to bypass intended authoriz

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from secalert@redhat.com

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

EPSS: 0.001520000 probability, percentile 0.358850000 (date 2026-04-07)

Problem Types: CWE-639 | CWE-255 | CWE-639 Authorization Bypass Through User-Controlled Key

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	CVSS	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
2.0	nvd@nist.gov	Primary	3.5		AV:N/AC:M/Au:S/C:N/I:P/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openstack	Essex	2012.1	All	All	All
Application	Openstack	Folsom	2012.2	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat OpenStack Platform 13 Queens	Not specified	Not specified
CNA	Red Hat	Red Hat OpenStack Platform 16.2	Not specified	Not specified
CNA	Red Hat	Red Hat OpenStack Platform 16.2	Not specified	Not specified
CNA	Red Hat	Red Hat OpenStack Platform 17.1	Not specified	Not specified
CNA	Red Hat	Red Hat OpenStack Platform 17.1	Not specified	Not specified
CNA	Red Hat	Red Hat OpenStack Platform 18.0	Not specified	Not specified
CNA	Red Hat	Red Hat OpenStack Platform 18.0	Not specified	Not specified

References

Reference	Source
oss-security - [OSSA 2012-019] Extension of token validity through token chaining (CVE-2012-5563)	af854a3a-2127-422b-91ae-364da2661
[SECURITY] Fedora 17 Update: openstack-keystone-2012.1.3-3.fc17	af854a3a-2127-422b-91ae-364da2661
Security Advisory SA51436 - Ubuntu update for keystone - Secunia	af854a3a-2127-422b-91ae-364da2661
access.redhat.com/security/cve/CVE-2012-5571	secalert@redhat.com
oss-security - [OSSA 2012-018] EC2-style credentials invalidation issue (CVE-2012-5571)	af854a3a-2127-422b-91ae-364da2661
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661
Ensures User is member of tenant in ec2 validation · openstack/keystone@9d68b40 · GitHub	af854a3a-2127-422b-91ae-364da2661
About Secunia Research | Flexera	af854a3a-2127-422b-91ae-364da2661
USN-1641-1: OpenStack Keystone vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364da2661
Bug #1064914 “Removing user from a tenant isn't invalidating use...” : Bugs : Keystone	af854a3a-2127-422b-91ae-364da2661
OpenStack Keystone CVE-2012-5571 Security Bypass Vulnerability	af854a3a-2127-422b-91ae-364da2661
Ensures User is member of tenant in ec2 validation · openstack/keystone@37308dd · GitHub	af854a3a-2127-422b-91ae-364da2661
Ensures User is member of tenant in ec2 validation · openstack/keystone@8735009 · GitHub	af854a3a-2127-422b-91ae-364da2661
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2026-04-02T15:02:50.229Z	Reported to Red Hat.
CNA	2012-12-18T01:00:00.000Z	Made public.

Legacy QID Mappings

996729 Python (Pip) Security Update for Keystone (GHSA-qvpr-qm6w-6rcc)

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