CVE-2017-2637

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

Summary

CVE	CVE-2017-2637
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-26 12:29:00 UTC
Updated	2023-02-12 23:29:00 UTC
Description	A design flaw issue was found in the Red Hat OpenStack Platform director use of TripleO to enable libvirtd based live-migra

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	10.0	All	All	All
Application	Redhat	Openstack	7.0	All	All	All
Application	Redhat	Openstack	8	All	All	All
Application	Redhat	Openstack	8.0	All	All	All
Application	Redhat	Openstack	9	All	All	All
Application	Redhat	Openstack	9.0	All	All	All
Application	Redhat	Openstack	10.0	All	All	All
Application	Redhat	Openstack	7.0	All	All	All
Application	Redhat	Openstack	8.0	All	All	All
Application	Redhat	Openstack	9.0	All	All	All

References

Reference	Source
Bug 1428240 – CVE-2017-2637 rhosp-director:libvirtd is deployed with no authentication	MISC
Red Hat OpenStack Platform director (TripleO) CVE-2017-2637 bug and Red Hat OpenStack Platform - Red Hat Customer Portal	CONFIRI
Red Hat Customer Portal	REDHAT

Red Hat Customer Portal	REDHAT
CVE-2017-2637 - Red Hat Customer Portal	MISC
OSSN/OSSN-0007 - OpenStack	CONFIR
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
Red Hat OpenStack Platform CVE-2017-2637 Remote Privilege Escalation Vulnerability	BID
1428240 – (CVE-2017-2637) CVE-2017-2637 rhosp-director:libvirtd is deployed with no authentication	CONFIR
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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