CVE-2017-1000256

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

Summary

CVE	CVE-2017-1000256
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-31 15:29:00 UTC
Updated	2023-11-07 02:37:00 UTC
Description	libvirt version 2.3.0 and later is vulnerable to a bad default configuration of "verify-peer=no" passed to QEMU by libvirt resul

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Redhat	Libvirt	All	All	All	All
Application	Redhat	Libvirt	All	All	All	All

References

Reference	Source	Link	Tag
Debian -- Security Information -- DSA-4003-1 libvirt	DEBIAN	www.debian.org	Thir
Bug#878799: CVE-2017-1000256/LSN-2017-0002: TLS certificate verification disabled for clients	MISC	www.mail-archive.com	Issu
[Libvirt-announce] LSN-2017-0002 - TLS certificate verification disabled	MLIST	www.redhat.com	Issu
CVE-2017-1000256 - Red Hat Customer Portal	CONFIRM	access.redhat.com	Issu
Bug#878799: CVE-2017-1000256/LSN-2017-0002: TLS certificate verification disabled for clients		www.mail-archive.com	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

900071 CBL-Mariner Linux Security Update for libvirt 6.1.0

902935 Common Base Linux Mariner (CBL-Mariner) Security Update for libvirt (2684)

905924 Common Base Linux Mariner (CBL-Mariner) Security Update for libvirt (2684-1)