CVE-2017-11334

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-11334
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-02 19:29:00 UTC
Updated	2020-11-10 18:32:00 UTC
Description	The address_space_write_continue function in exec.c in QEMU (aka Quick Emulator) allows local guest OS privileged user

Risk And Classification

Problem Types: CWE-125

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	Qemu	Qemu	All	All	All	All

References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party A
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party A
USN-3575-1: QEMU vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Party A
Bug 1471638 – CVE-2017-11334 Qemu: exec: oob access during dma operation	CONFIRM	bugzilla.redhat.com	Issue Tracki
oss-security - CVE-2017-11334 Qemu: exec: oob access during dma operation	MLIST	www.openwall.com	Mailing List,
[Qemu-devel] [PULL 21/41] exec: use qemu_ram_ptr_length to access guest	MLIST	lists.gnu.org	Mailing List,
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party A
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party A
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party A
QEMU CVE-2017-11334 Out of Bounds Read and Write Denial of Service Vulnerability	BID	www.securityfocus.com	Third Party A
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party A

Debian -- Security Information -- DSA-3925-1 qemu	DEBIAN	www.debian.org	Third Party A
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

900063 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0