CVE-2016-6888

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

Summary

CVE	CVE-2016-6888
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-10 00:59:09 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Integer overflow in the net_tx_pkt_init function in hw/net/net_tx_pkt.c in QEMU (aka Quick Emulator) allows local guest OS

Risk And Classification

Primary CVSS: v3.1 4.4 MEDIUM from nvd@nist.gov

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

EPSS: 0.000980000 probability, percentile 0.267000000 (date 2026-05-10)

Problem Types: CWE-190 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	2.1		AV:L/AC:L/Au:N/C:N/I:N/A:P

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

None

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Qemu	Qemu	2.7.0	rc0	All	All
Application	Qemu	Qemu	2.7.0	rc1	All	All
Application	Qemu	Qemu	2.7.0	rc2	All	All
Application	Qemu	Qemu	2.7.0	rc3	All	All
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	11	All	All	All
Application	Redhat	Openstack	6.0	All	All	All
Application	Redhat	Openstack	7.0	All	All	All
Application	Redhat	Openstack	8	All	All	All
Application	Redhat	Openstack	9	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Li
[SECURITY] [DLA 1599-1] qemu security update	af854a3a-2127-422b-91ae-364da2661108	lis
oss-security - Re: CVE Request: Qemu: net: vmxnet: integer overflow in packet initialisation	af854a3a-2127-422b-91ae-364da2661108	ww
[Qemu-devel] [PULL 1/2] net: vmxnet: use g_new for pkt initialisation	af854a3a-2127-422b-91ae-364da2661108	lis
oss-security - CVE Request: Qemu: net: vmxnet: integer overflow in packet initialisation	af854a3a-2127-422b-91ae-364da2661108	ww
QEMU: Multiple vulnerabilities (GLSA 201609-01) — Gentoo security	af854a3a-2127-422b-91ae-364da2661108	se
QEMU '/hw/net/net_tx_pkt.c' Integer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108	ww
git.qemu.org Git - qemu.git/commit	af854a3a-2127-422b-91ae-364da2661108	git
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108	ac
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108	ac
git.qemu.org Git - qemu.git/commit	MITRE	git
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

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