CVE-2015-3209

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

Summary

CVE	CVE-2015-3209
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-15 15:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Heap-based buffer overflow in the PCNET controller in QEMU allows remote attackers to execute arbitrary code by sending

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: CWE-787 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Arista	Eos	4.12	All	All	All

Operating System	Arista	Eos	4.13	All	All	All
Operating System	Arista	Eos	4.14	All	All	All
Operating System	Arista	Eos	4.15	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Application	Juniper	Junos Space	All	All	All	All
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Application	Redhat	Openstack	5.0	All	All	All
Application	Redhat	Virtualization	3.0	All	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp2	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	12	-	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	-	All	All

Vendor Declared Affected Products

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

References

Reference
QEMU: Arbitrary code execution (GLSA 201510-02) — Gentoo Security
XSA-135 - Xen Security Advisories
[security-announce] SUSE-SU-2015:1152-1: important: Security update for
[SECURITY] Fedora 20 Update: xen-4.3.4-6.fc20
[security-announce] SUSE-SU-2015:1206-1: important: Security update for
Arista - Security Advisory 0013
2017-04 Security Bulletin: Multiple Vulnerabilities in NorthStar Controller Application before version 2.1.0 Service Pack 1. - Juniper Networks
[security-announce] SUSE-SU-2015:1643-1: important: Security update for
[security-announce] SUSE-SU-2015:1045-1: important: Security update for
QEMU AMD PCnet Ethernet Emulation Heap Based Buffer Overflow Vulnerability
[security-announce] SUSE-SU-2015:1157-1: important: Security update for
Xen Heap Overflow in QEMU PCNET Controller Lets Local Guest Users Gain Privileges on the Host System - SecurityTracker
Red Hat Customer Portal
Debian -- Security Information -- DSA-3286-1 xen
[security-announce] SUSE-SU-2015:1426-1: important: Security update for
Juniper Networks - 2015-10 Security Bulletin: Junos Space: Multiple Vulnerabilities in Junos Space - Knowledge Base
Debian -- Security Information -- DSA-3284-1 qemu
[SECURITY] Fedora 21 Update: xen-4.4.2-6.fc21
[security-announce] SUSE-SU-2015:1042-1: important: Security update for
Red Hat Customer Portal
Red Hat Customer Portal
[SECURITY] Fedora 22 Update: xen-4.5.0-11.fc22
[security-announce] SUSE-SU-2015:1156-1: important: Security update for
Red Hat Customer Portal
Debian -- Security Information -- DSA-3285-1 qemu-kvm
Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security
[security-announce] SUSE-SU-2015:1519-1: important: Security update for
USN-2630-1: QEMU vulnerabilities | Ubuntu
Red Hat Customer Portal
Red Hat Customer Portal

Red Hat Customer Portal
Red Hat Customer Portal
access.redhat.com | CVE-2015-3209
Bug 1225882 – CVE-2015-3209 qemu: pcnet: multi-tmd buffer overflow in the tx path
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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