



CVE-2015-5165

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2015-5165
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-12 14:59:00 UTC
Updated	2023-02-13 00:50:00 UTC
Description	The C+ mode offload emulation in the RTL8139 network card device model in QEMU, as used in Xen 4.5.x and earlier, allo

Risk And Classification

Problem Types: CWE-908

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	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Oracle	Linux	7	0	All	All
Operating System	Redhat	Enterprise Linux Compute Node Eus	7.1	All	All	All
Operating System	Redhat	Enterprise Linux Compute Node Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Compute Node Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Compute Node Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Compute Node Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Compute Node Eus	7.6	All	All	All

Operating System	Redhat	Enterprise Linux Compute Node Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Eus Compute Node	6.7	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian	6.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian	7.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	6.7_ppc64	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.1_ppc64	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.2_ppc64	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.3_ppc64	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.4_ppc64	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.5_ppc64	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.6_ppc64	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.7_ppc64	All	All	All
Operating System	Redhat	Enterprise Linux For Scientific Computing	6.0	All	All	All
Operating System	Redhat	Enterprise Linux For Scientific Computing	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.1	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus From Rhui	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Server From Rhui	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server From Rhui	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All

Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Openstack	5.0	All	All	All
Application	Redhat	Openstack	6.0	All	All	All
Application	Redhat	Virtualization	3.0	All	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Xen	Xen	4.5.1	All	All	All
Operating System	Xen	Xen	4.5.1	All	All	All
Operating System	Xen	Xen	All	All	All	All

References

Reference

[SECURITY] Fedora 23 Update: xen-4.5.1-6.fc23

Red Hat Customer Portal

Red Hat Customer Portal

QEMU Realtek rtl8139 Model CVE-2015-5165 Information Disclosure Vulnerability

Arista - Security Advisory 0013

Debian -- Security Information -- DSA-3348-1 qemu

[SECURITY] Fedora 22 Update: xen-4.5.1-8.fc22

Red Hat Customer Portal

Red Hat Customer Portal

Red Hat Customer Portal

[security-announce] SUSE-SU-2015:1643-1: important: Security update for


Xen RTL8139 Device Model Memory Initialization Bug Lets Local Users on a Guest System Obtain Potentially Sensitive Information from the I

Red Hat Customer Portal

XSA-140 - Xen Security Advisories

Bug 1248760 – CVE-2015-5165 Qemu: rtl8139 uninitialized heap memory information leakage to guest (XSA-140)

Red Hat Customer Portal

Red Hat Customer Portal
Red Hat Customer Portal
access.redhat.com CVE-2015-5165
Oracle Linux Bulletin - October 2015
Debian -- Security Information -- DSA-3349-1 qemu-kvm
[SECURITY] Fedora 21 Update: xen-4.4.3-3.fc21
CVE-2015-5165 - Vulnerability in Citrix XenServer Could Result in Information Disclosure
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
[security-announce] SUSE-SU-2015:1421-1: important: Security update for
Red Hat Customer Portal
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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)