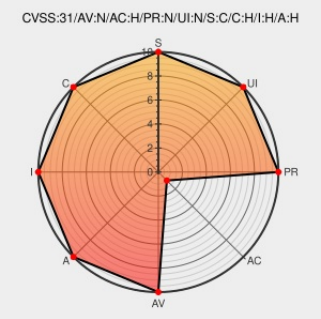
CVE-2015-7512

Published on: 01/08/2016 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:54:00 AM UTC

CVE-2015-7512

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

Buffer overflow in the pcnet_receive function in hw/net/pcnet.c in QEMU, when a guest NIC has a larger MTU, allows remote attackers to cause a denial of service (guest OS crash) or execute arbitrary code via a large packet.

CVE-2015-7512 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
git.qemu.org Git - qemu.git/commit	web.archive.org text/xml Inactive Link Not Archived	MISC git.qemu.org/?p=qemu.git%3Ba=commit%3Bh=8b98a2f07175d46c3f7217639bd5e03f
QEMU Buffer Overflow in AMD PC-	Third Party Advisory	SECTRACK 1034527

Net II Emulator Lets Remote Users Execute Arbitrary Code - SecurityTracker	VDB Entry www.securitytracker.com text/html	
Debian -- Security Information -- DSA-3471-1 qemu	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3471
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:2694
CVE-2015-7512 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2015-7512
QEMU 'hw/net/pcnet.c' Remote Buffer Overflow Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 78230
oss-security - CVE-2015-7512 Qemu: net: pcnet: buffer overflow in non-loopback mode	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20151130 CVE-2015-7512 Qemu: net: pcnet: buffer overflow in non-loopback mode
Debian -- Security Information -- DSA-3469-1 qemu	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3469
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:2696
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:2695
Debian -- Security Information -- DSA-3470-1 qemu-kvm	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3470
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2015:2696
Oracle Linux Bulletin - January 2016	Third Party Advisory www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2015:2695
Bug 1285061 – CVE-2015-7512 Qemu: net: pcnet: buffer overflow in non-loopback mode	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1285061
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2015:2694
QEMU: Multiple vulnerabilities (GLSA 201602-01) — Gentoo security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-201602-01

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	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	Oracle	Linux	6	-	All	All
Operating System	Oracle	Linux	6	-	All	All
Application	Qemu	Qemu	2.5.0	rc0	All	All
Application	Qemu	Qemu	2.5.0	rc1	All	All
Application	Qemu	Qemu	2.5.0	rc2	All	All
Application	Qemu	Qemu	2.5.0	rc0	All	All
Application	Qemu	Qemu	2.5.0	rc1	All	All
Application	Qemu	Qemu	2.5.0	rc2	All	All
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	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	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating	Redhat	Enterprise Linux Server	6.0	All	All	All

System						
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Application	Redhat	Openstack	5.0	All	All	All
Application	Redhat	Openstack	5.0	All	All	All
Application	Redhat	Virtualization	3.0	All	All	All
Application	Redhat	Virtualization	3.0	All	All	All

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:oracle:linux:6:-:*:*:*:*:*:*:

cpe:2.3:o:oracle:linux:6:-:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.5.0:rc0:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.5.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.5.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.5.0:rc0:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.5.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.5.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:*:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:6.7:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:6.7:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:virtualization:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:virtualization:3.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→