CVE-2015-3214

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-3214
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-31 10:59:00 UTC
Updated	2023-02-13 00:48:00 UTC
Description	The pit_ioport_read in i8254.c in the Linux kernel before 2.6.33 and QEMU before 2.3.1 does not distinguish between read

Risk And Classification

Problem Types: CWE-119

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	Lenovo	Emc Px12-400r Ivx	All	All	All	All
Operating System	Lenovo	Emc Px12-450r Ivx	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Qemu	Qemu	All	All	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 For Power Big Endian	7.0	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	7.0	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 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	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

References

References

Reference	Source	Link
Red Hat Customer Portal	MISC	access
CVE-2015-3214 - Red Hat Customer Portal	MISC	access
oss-security - Re: CVE request -- Linux kernel - kvm: x86: out-of-bounds memory access in pit_ioport_read function	MLIST	www.o
Arista - Security Advisory 0013	MISC	www.a
Red Hat Customer Portal	REDHAT	rhn.red
QEMU i8254 PIT Emulation Bug Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTRACK	www.s
Debian -- Security Information -- DSA-3348-1 qemu	DEBIAN	www.d
QEMU - Programmable Interrupt Timer Controller Heap Overflow - Multiple dos Exploit	EXPLOIT-DB	www.e
Bug 1229640 – CVE-2015-3214 qemu/kvm: i8254: out-of-bounds memory access in pit_ioport_read function	CONFIRM	bugzill
Re: [Qemu-devel] [PATCH] i8254: fix out-of-bounds memory access in pit_ioport_read()	MISC	www.m
QEMU 'pit_ioport_read()' Function Memory Corruption Vulnerability	BID	www.s
Re: [Qemu-devel] [PATCH] i8254: fix out-of-bounds memory access in pit_ioport_read()	MLIST	www.m
Red Hat Customer Portal	MISC	access
QEMU i8254 PIT Emulation Bug - Lenovo Support US	CONFIRM	suppor
QEMU i8254 PIT Emulation Bug - Lenovo Support (US)	CONFIRM	suppor
404 Not Found	CONFIRM	mirror.l
Red Hat Customer Portal	REDHAT	rhn.red
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kern
Red Hat Customer Portal	MISC	access
Red Hat Customer Portal	REDHAT	rhn.red
KVM: PIT: control word is write-only · torvalds/linux@ee73f65 · GitHub	CONFIRM	github.c
QEMU: Arbitrary code execution (GLSA 201510-02) — Gentoo Security	GENTOO	securit
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nis

No vendor comments have been submitted for this CVE.

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

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report