CVE-2014-3647

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

Summary

CVE	CVE-2014-3647
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-10 11:55:00 UTC
Updated	2023-02-13 00:41:00 UTC
Description	arch/x86/kvm/emulate.c in the KVM subsystem in the Linux kernel through 3.17.2 does not properly perform RIP changes, v

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Opensuse	Evergreen	11.4	All	All	All
Operating System	Opensuse	Evergreen	11.4	All	All	All
Operating System	Oracle	Linux	7	-	All	All
Operating System	Oracle	Linux	7	-	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp2	All	All

References

Reference	Source	Link
Linux Kernel KVM CVE-2014-3647 Local Denial of Service Vulnerability	BID	www.securityfocus.com
CVE-2014-3647 - Red Hat Customer Portal	MISC	access.redhat.com
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
USN-2417-1: Linux kernel vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com
KVM: x86: Emulator fixes for eip canonical checks on near branches · torvalds/linux@234f3ce · GitHub	CONFIRM	github.com
Debian -- Security Information -- DSA-3060-1 linux	DEBIAN	www.debian.org
Bug 1144897 – CVE-2014-3647 kernel: kvm: noncanonical rip after emulation	CONFIRM	bugzilla.redhat.com
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
[security-announce] openSUSE-SU-2015:0566-1: important: kernel update fo	SUSE	lists.opensuse.org
Oracle Linux Bulletin - October 2015	CONFIRM	www.oracle.com
[security-announce] SUSE-SU-2015:0481-1: important: Security update for	SUSE	lists.opensuse.org
USN-2418-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com
Red Hat Customer Portal	MISC	access.redhat.com
USN-2394-1: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com
KVM: x86: Handle errors when RIP is set during far jumps · torvalds/linux@d1442d8 · GitHub	CONFIRM	github.com
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
oss-security - kvm issues	MLIST	www.openwall.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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