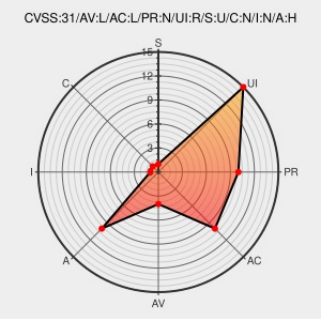
CVE-2014-3646

Published on: 11/10/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:41:00 AM UTC

CVE-2014-3646

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

arch/x86/kvm/vmx.c in the KVM subsystem in the Linux kernel through 3.17.2 does not have an exit handler for the INVVPID instruction, which allows guest OS users to cause a denial of service (guest OS crash) via a crafted application.

CVE-2014-3646 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.7 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Red Hat Customer Portal	Third Party Advisory, web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2015:0126

USN-2417-1: Linux kernel vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2417-1
Debian -- Security Information -- DSA-3060-1 linux	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3060
Bug 1144825 – CVE-2014-3646 kernel: kvm: vmx: invvpid vm exit not handled	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1144825
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:0284
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2015:0284
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2015:0126
access.redhat.com | CVE-2014-3646	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2014-3646
kvm: vmx: handle invvpid vm exit gracefully · torvalds/linux@a642fc3 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/a642fc305053cc1c6e47e4f4df327895747ab485
[security-announce] openSUSE-SU-2015:0566-1: important: kernel update fo	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2015:0566
[security-announce] SUSE-SU-2015:0481-1: important: Security update for	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SU-2015:0481
USN-2418-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2418-1
USN-2394-1: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2394-1
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2014:1843
kernel/git/torvalds/linux.git - Linux kernel source tree	web.archive.org text/html Inactive Link Not Archived	MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=a642fc305053cc1c6e47e4f4df327895747ab485
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2014:1724
oss-security - kvm issues	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20141024 kvm issues

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	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	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	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

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:

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

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

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:evergreen:11.4:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:evergreen:11.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:11:sp2:*:*:ltss:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:11:sp2:*:*:ltss:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→