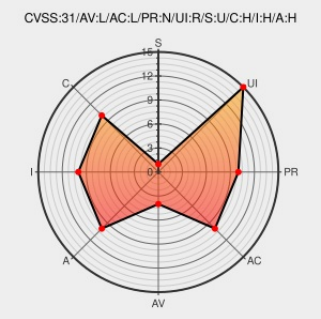
CVE-2013-1943

Published on: 07/16/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:42:00 AM UTC

CVE-2013-1943

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



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

The KVM subsystem in the Linux kernel before 3.0 does not check whether kernel addresses are specified during allocation of memory slots for use in a guest's physical address space, which allows local users to gain privileges or obtain sensitive information from kernel memory via a crafted application, related to arch/x86/kvm/paging_tmpl.h and virt/kvm/kvm_main.c.

CVE-2013-1943 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 4.4 - MEDIUM

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

CVE References

Description	Tags	Link
	Broken Link web.archive.org	CONFIRM web.archive.org/web/20130329070349/ftp.osuosl.org/pub/linux/kernel/v3.0/ChangeL

	text/plain	3.0
access.redhat.com | CVE-2013-1943	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2013-1943
kernel/git/torvalds/linux.git - Linux kernel source tree	Mailing List Patch Vendor Advisory 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=fa3d315a4ce2c0891cdde262562e710d95fba19e
Bug 950490 – CVE-2013-1943 kernel: kvm: missing check in kvm_set_memory_region()	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=950490
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2013:0911
KVM: Validate userspace_addr of memslot when registered · torvalds/linux@fa3d315 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/fa3d315a4ce2c0891cdde262562e710d95fba19e
USN-1939-1: Linux kernel vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-1939-1

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	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	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	Redhat	Enterprise Linux Eus	6.2	All	All	All

Operating System	Redhat	Enterprise Linux Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.2	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.3	All	All	All

- cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:
- cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux:5.0:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux:5.0:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_eus:6.2:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_eus:6.3:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_eus:6.2:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_eus:6.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→