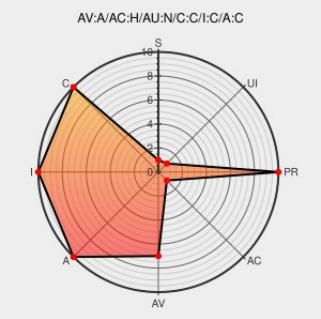
CVE-2013-1797

Published on: 03/22/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:41:00 AM UTC

CVE-2013-1797

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



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

Use-after-free vulnerability in arch/x86/kvm/x86.c in the Linux kernel through 3.8.4 allows guest OS users to cause a denial of service (host OS memory corruption) or possibly have unspecified other impact via a crafted application that triggers use of a guest physical address (GPA) in (1) movable or (2) removable memory during an MSR_KVM_SYSTEM_TIME kvm_set_msr_common operation.

CVE-2013-1797 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
oss-security - linux kernel: kvm: CVE-2013-179[6..8]	www.openwall.com text/html	MLIST [oss-security] 20130320 linux kernel: kvm: CVE-2013-179[6..8]
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0727
KVM: x86: Convert MSR_KVM_SYSTEM_TIME to use gfn_to_hva_cache functio… · torvalds/linux@0b79459 · GitHub	github.com text/html	CONFIRM github.com/torvalds/linux/commit/0b79459b482e85cb7426aa7da683a9f2c97aeae1

[security-announce] openSUSE-SU-2013:1187-1: important: 3.0.80 kernel up	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1187
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2013:1026
[security-announce] openSUSE-SU-2013:0925-1: important: kernel: security	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0925
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=0b79459b482e85cb7426aa7da683a9f2c97aeae1
access.redhat.com | CVE-2013-1797	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2013-1797
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0744
917013 – (CVE-2013-1797) CVE-2013-1797 kernel: kvm: after free issue with the handling of MSR_KVM_SYSTEM_TIME	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=917013
USN-1809-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1809-1
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0928
USN-1812-1: Linux kernel (Quantal HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1812-1
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0746
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2013:0744
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1026
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2013:0727
Support / Security / Advisories / / MDVSA-2013:176 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2013:176
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2013:0746
[security-announce] openSUSE-SU-2013:0847-1: important: kernel: security	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0847
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2013:0928

USN-1813-1: Linux kernel vulnerabilities | Ubuntu www.ubuntu.com text/html UBUNTU USN-1813-1

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	Linux	Linux Kernel	3.8.0	All	All	All
Operating System	Linux	Linux Kernel	3.8.1	All	All	All
Operating System	Linux	Linux Kernel	3.8.2	All	All	All
Operating System	Linux	Linux Kernel	3.8.3	All	All	All
Operating System	Linux	Linux Kernel	3.8.0	All	All	All
Operating System	Linux	Linux Kernel	3.8.1	All	All	All
Operating System	Linux	Linux Kernel	3.8.2	All	All	All
Operating System	Linux	Linux Kernel	3.8.3	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:3.8.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.3:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→