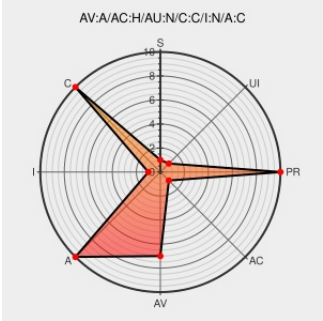
CVE-2013-1798

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

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

CVE-2013-1798

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



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

The ioapic_read_indirect function in virt/kvm/ioapic.c in the Linux kernel through 3.8.4 does not properly handle a certain combination of invalid IOAPIC_REG_SELECT and IOAPIC_REG_WINDOW operations, which allows guest OS users to obtain sensitive information from host OS memory or cause a denial of service (host OS OOPS) via a crafted application.

CVE-2013-1798 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.2 - MEDIUM

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	NONE	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
[security-announce] openSUSE-SU-2013:1187-1: important: 3.0.80 kernel up	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1187
kernel/git/torvalds/linux.git - Linux kernel source tree	web.archive.org text/html	MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=a2c118bfab8bc6b8bb213abfc35201e441693d55

	Inactive Link Not Archived	
[security-announce] openSUSE-SU-2013:0925-1: important: kernel: security	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0925
917017 – (CVE-2013-1798) CVE-2013-1798 kernel: kvm: out-of-bounds access in ioapic indirect register reads	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=917017
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0744
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	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1026
Kernel Live Patch Security Notice LSN-0065-1 ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/157233/Kernel-Live-Patch-Security-Notice-LSN-0065-1.html
Support / Security / Advisories / / MDVSA-2013:176 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2013:176
KVM: Fix bounds checking in ioapic indirect register reads (CVE-2013-… · torvalds/linux@a2c118b · GitHub	Exploit Patch github.com text/html	CONFIRM github.com/torvalds/linux/commit/a2c118bfab8bc6b8bb213abfc35201e441693d55
[security-announce] openSUSE-SU-2013:0847-1: important: kernel: security	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0847
USN-1813-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1813-1

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	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→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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