

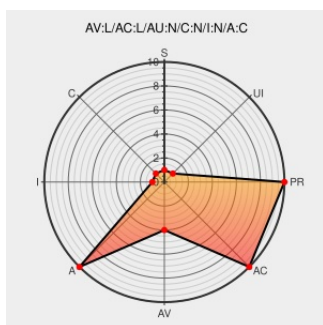


CVE-2010-3067

Published on: 09/21/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:21:00 AM UTC

CVE-2010-3067

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

Integer overflow in the do_io_submit function in fs/aio.c in the Linux kernel before 2.6.36-rc4-next-20100915 allows local users to cause a denial of service or possibly have unspecified other impact via crafted use of the io_submit system call.

CVE-2010-3067 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4.9 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

SUSE update for kernel -
Advisories - Community

[Third Party Advisory](#)
[web.archive.org](#)
[text/html](#)

[SECUNIA 42801](#)

[security-announce] SUSE
Security Announcement:
Realtime Linux Kernel (S

[Mailing List](#)
[Third Party Advisory](#)
[lists.opensuse.org](#)
[text/html](#)

[SUSE SUSE-SA:2011:007](#)

SUSE update for kernel -
Advisories - Community

[Third Party Advisory](#)
[web.archive.org](#)
[text/html](#)

[SECUNIA 43291](#)

Webmail : Solution de
messagerie professionnelle -
OVHcloud- OVH

[Third Party Advisory](#)
[www.vupen.com](#)
[text/html](#)

[VUPEN ADV-2011-0375](#)

Support	Third Party Advisory www.redhat.com text/html	 REDHAT RHSA-2010:0779
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SA:2011:002
Support	Third Party Advisory www.redhat.com text/html	 REDHAT RHSA-2010:0758
SecurityFocus	Third Party Advisory VDB Entry www.securityfocus.com text/html	 BUGTRAQ 20111013 VMSA-2011-0012 VMware ESXi and ESX updates to third party libraries and ESX Service Console
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	 VUPEN ADV-2011-0012
IBM X-Force Exchange	Third Party Advisory VDB Entry exchange.xforce.ibmcloud.com text/html	 XF kernel-doiosubmit-dos(61884)
USN-1000-1: Linux kernel vulnerabilities Ubuntu	Third Party Advisory www.ubuntu.com text/html	 UBUNTU USN-1000-1
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=75e1c70fc31490ef8a373ea2a4bea2524099b478
Support	Third Party Advisory www.redhat.com text/html	 REDHAT RHSA-2010:0839
SUSE update for kernel - Advisories - Community	Third Party Advisory web.archive.org text/html	 SECUNIA 42778
mandriva.com	Third Party Advisory www.mandriva.com text/html	 MANDRIVA MDVSA-2011:029
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SA:2010:060
VMSA-2011-0012.2	Third Party Advisory www.vmware.com text/html	 CONFIRM www.vmware.com/security/advisories/VMSA-2011-0012.html
Support / Security / Advisories // MDVSA-2010:257 Mandriva	Third Party Advisory www.mandriva.com text/html	 MANDRIVA MDVSA-2010:257
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SA:2011:001
Red Hat update for kernel - Advisories - Community	Third Party Advisory web.archive.org text/html	 SECUNIA 42890

	text/html	
About Secunia Research Flexera	Third Party Advisory secunia.com Deprecated Link text/plain	 SECUNIA 46397
Debian -- Security Information -- DSA-2126-1 linux-2.6	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-2126
Bug 629441 – CVE-2010-3067 kernel: do_io_submit() infoleak	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=629441
mandriva.com	Third Party Advisory www.mandriva.com text/html	 MANDRIVA MDVSA-2011:051
access.redhat.com	Third Party Advisory www.redhat.com text/html	 REDHAT RHSA-2011:0007
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	 VUPEN ADV-2011-0298
404: File not found	Broken Link www.kernel.org text/html Inactive Link Not Archived	 CONFIRM www.kernel.org/pub/linux/kernel/v2.6/next/patch-v2.6.36-rc4-next-20100915.bz2
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SA:2011:008
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	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All

Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	2.6.36	-	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc3	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	2.6.36	-	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc3	All	All
Operating System	Opensuse	Opensuse	11.2	All	All	All
Operating System	Opensuse	Opensuse	11.3	All	All	All
Operating System	Opensuse	Opensuse	11.2	All	All	All
Operating System	Opensuse	Opensuse	11.3	All	All	All

Operating System	Suse	Linux Enterprise Desktop	10	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp3	All	All
Operating System	Suse	Linux Enterprise Real Time Extension	11	sp1	All	All
Operating System	Suse	Linux Enterprise Real Time Extension	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	10	sp3	All	All
Operating System	Suse	Linux Enterprise Server	9	All	All	All
Operating System	Suse	Linux Enterprise Server	10	sp3	All	All
Operating System	Suse	Linux Enterprise Server	9	All	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	10	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	10	sp3	All	All
cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:10.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:6.06:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:8.04:*:*:*:-:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:9.04:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:9.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:10.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:6.06:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:8.04:*:*:*:-:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:9.04:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:9.10:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.36:-:*:*:*:*:						

cpe:2.3:o:linux:linux_kernel:2.6.36:rc1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.36:rc2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.36:rc3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.36:-:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.36:rc1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.36:rc2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.36:rc3:*:*:*:*:*:
cpe:2.3:o:opensuse:opensuse:11.2:*:*:*:*:*:
cpe:2.3:o:opensuse:opensuse:11.3:*:*:*:*:*:
cpe:2.3:o:opensuse:opensuse:11.2:*:*:*:*:*:
cpe:2.3:o:opensuse:opensuse:11.3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_desktop:10:sp3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_desktop:10:sp3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_real_time_extension:11:sp1:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_real_time_extension:11:sp1:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:10:sp3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:9:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:10:sp3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:9:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_software_development_kit:10:sp3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_software_development_kit:10:sp3:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

CVE, CWE, and OVAL are registered 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](#)