



# CVE-2009-3547

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2009-3547
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-11-04 15:30:00 UTC
<b>Updated</b>	2023-11-03 17:14:00 UTC
<b>Description</b>	Multiple race conditions in fs/pipe.c in the Linux kernel before 2.6.32-rc6 allow local users to cause a denial of service (NUL

## Risk And Classification

**Problem Types:** CWE-362 | CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	6.06	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	8.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	8.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	9.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	9.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	6.06	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	8.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	8.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	9.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	9.10	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	10	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	10	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.32	-	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.32	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.32	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.32	rc3	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.32	rc4	All	All

Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.32	rc5	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.32	-	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.32	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.32	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.32	rc3	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.32	rc4	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.32	rc5	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Linux Desktop</a>	9	All	All	All
Operating System	<a href="#">Novell</a>	<a href="#">Linux Desktop</a>	9	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	11.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	11.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	11.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	11.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	3.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	5.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	4.8	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	5.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	3.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	5.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	3.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	5.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Mrg Realtime</a>	1.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Desktop</a>	10	sp2	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Desktop</a>	10	sp2	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Server</a>	10	sp2	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Server</a>	10	sp2	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esx</a>	4.0	All	All	All
Operating System	<a href="#">Vmware</a>	<a href="#">Esx</a>	4.0	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Vma</a>	4.0	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Vma</a>	4.0	All	All	All

## References

Reference	So
access.redhat.com   CVE-2009-3547	MI:
Red Hat Customer Portal	MI:
Repository / Oval Repository	OV
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SU
Repository / Oval Repository	OV
rhn.redhat.com   Red Hat Support	RE
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VU
[SECURITY] Fedora 10 Update: kernel-2.6.27.38-170.2.113.fc10	FE
Red Hat Customer Portal	MI:
Support	RE
USN-864-1: Linux kernel vulnerabilities   Ubuntu	UB
LKML: Earl Chew: fs/pipe.c null pointer dereference	ML
Support / Security / Advisories // MDVSA-2009:329   Mandriva	MA
rhn.redhat.com   Red Hat Support	RE
rhn.redhat.com   Red Hat Support	RE
Repository / Oval Repository	OV
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SU
SUSE update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	SE
Red Hat Customer Portal	MI:
Red Hat Customer Portal	MI:
LKML: =?UTF-8?Q?Am=C3=A9rico_Wang?=: Re: [PATCH v4 1/1]: fs: pipe.c null pointer dereference + really sign off + unmangled diffs	ML
SUSE update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	SE
kernel/git/torvalds/linux.git - Linux kernel source tree	MI:
404: File not found	CC
530490 – (CVE-2009-3547) CVE-2009-3547 kernel: fs: pipe.c null pointer dereference	CC
Red Hat Customer Portal	RE
Red Hat Customer Portal	MI:
VMware vMA Update for Multiple Packages - Advisories - Community	SE
'[oss-security] CVE-2009-3547 kernel: fs: pipe.c null pointer dereference' - MARC	ML
Red Hat Customer Portal	MI:
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SU
SecurityFocus	BU
[Security-announce] VMSA-2010-0004 ESX Service Console and vMA third party updates	ML
Linux Kernel 'pipe.c' Local Privilege Escalation Vulnerability	BI

kernel/git/torvalds/linux.git - Linux kernel source tree	CC
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SU
Red Hat Customer Portal	MI
VMware ESX Server 4 Multiple Vulnerabilities - Advisories - Community	SE
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)**