



CVE-2009-1072

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

Summary

CVE	CVE-2009-1072
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-03-25 01:30:00 UTC
Updated	2023-11-07 02:03:00 UTC
Description	nfsd in the Linux kernel before 2.6.28.9 does not drop the CAP_MKNOD capability before handling a user request in a three

Risk And Classification

Problem Types: CWE-16

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	8.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	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	8.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	4.0	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	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Opensuse	Opensuse	10.3	All	All	All

Operating System	Opensuse	Opensuse	11.0	All	All	All
Operating System	Opensuse	Opensuse	11.1	All	All	All
Operating System	Opensuse	Opensuse	10.3	All	All	All
Operating System	Opensuse	Opensuse	11.0	All	All	All
Operating System	Opensuse	Opensuse	11.1	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	Suse	Linux Enterprise Desktop	10	sp2	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp2	All	All
Operating System	Suse	Linux Enterprise Server	10	sp2	All	All
Operating System	Suse	Linux Enterprise Server	10	sp2	All	All
Operating System	Vmware	Esx	3.0.3	All	All	All
Operating System	Vmware	Esx	3.5	All	All	All
Operating System	Vmware	Esx	4.0	All	All	All
Operating System	Vmware	Esx	3.0.3	All	All	All
Operating System	Vmware	Esx	3.5	All	All	All
Operating System	Vmware	Esx	4.0	All	All	All
Application	Vmware	Server	2.0.0	All	All	All
Application	Vmware	Server	2.0.0	All	All	All
Application	Vmware	Vcenter Server	4.0	-	All	All
Application	Vmware	Vcenter Server	4.0	-	All	All
Application	Vmware	Virtualcenter	2.0.2	All	All	All
Application	Vmware	Virtualcenter	2.5	All	All	All
Application	Vmware	Virtualcenter	2.0.2	All	All	All
Application	Vmware	Virtualcenter	2.5	All	All	All
Application	Vmware	Vma	4.0	All	All	All
Application	Vmware	Vma	4.0	All	All	All

References

Reference	Source	Link
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.o
oss-security - CVE request: kernel: nfsd did not drop CAP_MKNOD for non-root	MLIST	www.
Linux Kernel nfsd 'CAP_MKNOD' Unauthorized Access Vulnerability	BID	www.
SUSE update for kernel - Secunia.com	SECUNIA	secur
Gmane Loom	MLIST	threa
USN-700-1: Linux kernel: nfsd did not drop CAP_MKNOD for non-root	USN	www.

USN-793-1: Linux kernel vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
Repository / Oval Repository	OVAL	oval.mitre.org
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Ubuntu update for linux and linux-source-2.6.15 - Secunia.com	SECUNIA	secunia.com
Security Advisory SA35390 - SUSE update for kernel - Secunia	SECUNIA	secunia.com
Linux Kernel nfsd "CAP_MKNOD" Security Bypass - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
SecurityFocus	BUGTRAQ	www.securityfocus.com
Repository / Oval Repository	OVAL	oval.mitre.org
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:2009-0016)	SUSE	lists.suse.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.ovh.com
SUSE update for kernel - Secunia.com	SECUNIA	secunia.com
SUSE update for kernel - Secunia.com	SECUNIA	secunia.com
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:2009-0016)	SUSE	lists.suse.com
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:2009-0016)	SUSE	lists.suse.com
Red Hat update for kernel-rt - Secunia.com	SECUNIA	secunia.com
404: File not found	CONFIRM	www.ubuntu.com
Debian update for linux-2.6 - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
Support	REDHAT	www.redhat.com
VMSA-2009-0016.1	CONFIRM	www.ubuntu.com
kernel/git/torvalds/linux.git - Linux kernel source tree		git.kernel.org
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.ovh.com
Linux Kernel Information Disclosure and Security Bypass - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
VMware ESX and vMA Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
Debian -- Security Information -- DSA-1800-1 linux-2.6	DEBIAN	www.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-09-10	Tomas Hoger	This issue has been rated as having moderate security impact. It was addressed in Red Hat Er

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

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](#)