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 threa

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-793-1: Linux kernel vulnerabilities | Ubuntu	UBUNTU	www.
Repository / Oval Repository	OVAL	oval.c
IBM X-Force Exchange	XF	excha
Ubuntu update for linux and linux-source-2.6.15 - Secunia.com	SECUNIA	secur
Security Advisory SA35390 - SUSE update for kernel - Secunia	SECUNIA	secur
Linux Kernel nfsd "CAP_MKNOD" Security Bypass - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secur
SecurityFocus	BUGTRAQ	www.
Repository / Oval Repository	OVAL	oval.c
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.o
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.
SUSE update for kernel - Secunia.com	SECUNIA	secur
SUSE update for kernel - Secunia.com	SECUNIA	secur
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.o
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.o
Red Hat update for kernel-rt - Secunia.com	SECUNIA	secur
404: File not found	CONFIRM	www.
Debian update for linux-2.6 - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secur
Support	REDHAT	www.
VMSA-2009-0016.1	CONFIRM	www.
kernel/git/torvalds/linux.git - Linux kernel source tree		git.ke
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.ke
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.
Linux Kernel Information Disclosure and Security Bypass - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secur
VMware ESX and vMA Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secur
Debian -- Security Information -- DSA-1800-1 linux-2.6	DEBIAN	www.
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

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.

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