CVE-2008-2931

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2008-2931
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-07-09 18:41:00 UTC
Updated	2023-02-13 02:19:00 UTC
Description	The do_change_type function in fs/namespace.c in the Linux kernel before 2.6.22 does not verify that the caller has the CA

Risk And Classification

Problem Types: CWE-269

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	7.04	All	All	All
Operating System	Canonical	Ubuntu Linux	7.10	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	7.04	All	All	All
Operating System	Canonical	Ubuntu Linux	7.10	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	10.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	10.0	sp2	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	10.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	10.0	sp2	All	All
Operating System	Novell	Suse Linux Enterprise Server	10.0	sp1	All	All

Operating System	Novell	Suse Linux Enterprise Server	10.0	sp2	All	All
Operating System	Novell	Suse Linux Enterprise Server	10.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Server	10.0	sp2	All	All
Operating System	Opensuse	Opensuse	All	All	All	All

References

Reference	Source	Link
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.opensuse.org
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:025	SUSE	lists.opensuse.org
oss-security - Re: CVE-2008-2931 kernel: missing check before setting mount propagation	MLIST	www.openwall.com
Debian update for linux-2.6 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
404: File not found	CONFIRM	kernel.org
Bug 454388 – CVE-2008-2931 kernel: missing check before setting mount propagation	CONFIRM	bugzilla.redhat.com
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
Red Hat update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
Ubuntu update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
Support	REDHAT	www.redhat.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.
Repository / Oval Repository	OVAL	oval.cisecurity.org
SUSE update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.opensuse.org
USN-637-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
Debian -- Security Information -- DSA-1630-1 linux-2.6	DEBIAN	www.debian.org
oss-security - CVE-2008-2931 kernel: missing check before setting mount propagation	MLIST	www.openwall.com
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.opensuse.org
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
Linux Kernel 'do_change_type()' Local Security Bypass Vulnerability	BID	www.securityfocus.com
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	2009-01-15	Tomas Hoger	This issue did not affect the versions of Linux kernel as shipped with Red Hat Enterprise Linux

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

Free CVE JSON API cve.report/api

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