CVE-2008-4210

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

Summary

CVE	CVE-2008-4210
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-09-29 17:17:00 UTC
Updated	2023-11-07 02:02:00 UTC
Description	fs/open.c in the Linux kernel before 2.6.22 does not properly strip setuid and setgid bits when there is a write to a file, which

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.2.27	All	All	All
Operating System	Linux	Linux Kernel	2.4.36	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.1	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.2	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.3	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.4	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.5	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.6	All	All	All
Operating System	Linux	Linux Kernel	2.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc7	All	All

Operating System	Linux	Linux Kernel	2.6.19.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.19	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.20	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.21	All	All	All
Operating System	Linux	Linux Kernel	2.6.21.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.21.6	All	All	All
Operating System	Linux	Linux Kernel	2.2.27	All	All	All
Operating System	Linux	Linux Kernel	2.4.36	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.1	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.2	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.3	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.4	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.5	All	All	All
Operating System	Linux	Linux Kernel	2.4.36.6	All	All	All
Operating System	Linux	Linux Kernel	2.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.18	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.19.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.17	All	All	All

Operating System	Linux	Linux Kernel	2.6.20.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.19	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.20	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.21	All	All	All
Operating System	Linux	Linux Kernel	2.6.21.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.21.6	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:025	SUSE	lists.o
Repository / Oval Repository	OVAL	oval.c
git.kernel.org		git.ker
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secun
404: File not found	CONFIRM	kernel
[security-announce] SUSE Security Announcement: Kernel (SUSE-SA:2008:056	SUSE	lists.o
rhn.redhat.com | Red Hat Support	REDHAT	rhn.re
Red hat update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secun
Support / Security / Advisories / / MDVSA-2008:220 | Mandriva	MANDRIVA	www.r
Debian -- Security Information -- DSA-1653-1 linux-2.6	DEBIAN	www.d
Support	REDHAT	www.r
oss-security - Re: CVE request: kernel: open() call allows setgid bit when user is not in new file's group	MLIST	www.o
Ubuntu update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secun
Red Hat update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secun
Red Hat update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secun
git.kernel.org	CONFIRM	git.ker
Repository / Oval Repository	OVAL	oval.c
Support	REDHAT	www.r
404: File not found	CONFIRM	www.k
Linux Kernel Denial of Service and Privilege Escalation - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secun
Bug 8420 – open() call allows setgid bit when user is not in new file's group	CONFIRM	bugzil
IBM X-Force Exchange	XF	excha
Debian update for linux-2.6 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secun
oss-security - CVE request: kernel: open() call allows setgid bit when user is not in new file's group	MLIST	www.o
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.o
Support	REDHAT	www.r

[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.o
Red Hat update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secun
USN-679-1: Linux kernel vulnerabilities | Ubuntu	UBUNTU	www.u
Linux Kernel 'truncate()' Local Privilege Escalation Vulnerability	BID	www.s
SUSE update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secun
Bug 463661 – CVE-2008-4210 kernel: open() call allows setgid bit when user is not in new file's group	CONFIRM	bugzil
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

No vendor comments have been submitted for this CVE.

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