CVE-2008-0009

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

Summary

CVE	CVE-2008-0009
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-02-12 21:00:00 UTC
Updated	2018-10-15 21:57:00 UTC
Description	The vmsplice_to_user function in fs/splice.c in the Linux kernel 2.6.22 through 2.6.24 does not validate a certain userspace

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.22	All	All	All
Operating System	Linux	Linux Kernel	2.6.22	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.22.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.23	All	All	All
Operating System	Linux	Linux Kernel	2.6.23	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.23	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.23.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.4	All	All	All

Operating System	Linux	Linux Kernel	2.6.23.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.24	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.24	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.22	All	All	All
Operating System	Linux	Linux Kernel	2.6.22	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.22.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.22.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.23	All	All	All
Operating System	Linux	Linux Kernel	2.6.23	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.23	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.23.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.24	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.24	rc3	All	All

References

Reference	Source	Link
404: File not found	CONFIRM	www.kern
SecurityFocus	BUGTRAQ	www.secu
Bug 431206 – CVE-2008-0009 kernel: Inappropriate dereference of user-supplied memory pointers	CONFIRM	bugzilla.re

Linux Kernel Prior to 2.6.24.1 'vmsplice_to_user()' Local Privilege Escalation Vulnerability	BID	www.secu
Linux Kernel "vmsplice()" System Call Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.c
isec.pl/vulnerabilities/isec-0026-vmsplice_to_kernel.txt	MISC	isec.pl
Webmail - OVH	VUPEN	www.vupe
[SECURITY] Fedora 7 Update: kernel-2.6.23.15-80.fc7	FEDORA	www.redh
[SECURITY] Fedora 8 Update: kernel-2.6.23.15-137.fc8	FEDORA	www.redh
RETIRED: Linux Kernel Multiple Prior to 2.6.24.1 Multiple Memory Access Vulnerabilities	BID	www.secu
Fedora update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.c
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2008-02-13	Mark J Cox	Not vulnerable. This issue did not affect the versions of the Linux kernel as shipped with Red Ha

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