CVE-2011-2182

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

Summary

CVE	CVE-2011-2182
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-13 10:24:00 UTC
Updated	2023-11-07 02:07:00 UTC
Description	The ldm_frag_add function in fs/partitions/ldm.c in the Linux kernel before 2.6.39.1 does not properly handle memory alloca

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.39	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.39	rc7	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
Linux Kernel LDM Partition Heap Based Buffer Overflow Vulnerability	BID	www.secu
404 Not Found	CONFIRM	ftp.osuosl.
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.c
Fix for buffer overflow in ldm_frag_add not sufficient · torvalds/linux@cae13fe · GitHub	CONFIRM	github.com
'[security bulletin] HPSBGN02970 rev.1 - HP Rapid Deployment Pack (RDP) or HP Insight Control Server ' - MARC	HP	marc.info
oss-security - Re: CVE request: kernel: fs/partitions: Kernel heap overflow via corrupted LDM partition tables	MLIST	www.open
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.c
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

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