



CVE-2011-1012

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2011-1012
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-03-01 23:00:00 UTC
Updated	2023-02-13 01:18:00 UTC
Description	The ldm_parse_vmdb function in fs/partitions/ldm.c in the Linux kernel before 2.6.38-rc6-git6 does not validate the VBLK size

Risk And Classification

Problem Types: CWE-369

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	2.6.38	-	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc5	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	2.6.38	-	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc5	All	All

References		
Reference	Source	Link
USN-1146-1: Linux kernel vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com/usn/USN-1146-1
oss-security - CVE request: kernel: Corrupted LDM partition table issues	MLIST	openwall.com/lists/oss-security/2011/01/01/1
www.pre-cert.de/advisories/PRE-SA-2011-01.txt	MISC	www.pre-cert.de/advisories/PRE-SA-2011-01.txt
404: File not found	CONFIRM	www.kernel.org
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
oss-security - Re: CVE request: kernel: Corrupted LDM partition table issues	MLIST	openwall.com/lists/oss-security/2011/01/01/1
Linux Kernel Divide By Zero Error in ldm_get_vblks() Lets Physically Local Users Deny Service - SecurityTracker	SECTRAK	www.securitytracker.com
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
Linux Kernel 'fs/partitions/ldm.c' Buffer Overflow and Denial of Service Vulnerabilities	BID	www.securityfocus.com/bid/404
Linux Kernel Buffer Overflow ldm_frag_add() Elevated Privileges - SecurityReason.com	SREASON	securityreason.com
SecurityFocus	BUGTRAQ	www.securityfocus.com
+ ldm-corrupted-partition-table-can-cause-kernel-oops.patch added to -mm tree -- MM Commits	MLIST	www.spinics.net
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
No vendor comments have been submitted for this CVE.		
There are currently no legacy QID mappings associated with this CVE.		