CVE-2011-1017

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

Summary

CVE	CVE-2011-1017
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-03-01 23:00:00 UTC
Updated	2020-08-07 19:28:00 UTC
Description	Heap-based buffer overflow in the ldm_frag_add function in fs/partitions/ldm.c in the Linux kernel 2.6.37.2 and earlier might

Risk And Classification

Problem Types: CWE-787

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	All	All	All	All

References

Reference	Source	Link
Linux Kernel Buffer Overflow in ldm_frag_add() May Let Local Users Gain Elevated Privileges - SecurityTracker	SECTRACK	securitytrack
USN-1146-1: Linux kernel vulnerabilities | Ubuntu	UBUNTU	www.ubuntu
oss-security - Re: CVE request: kernel: fs/partitions: Kernel heap overflow via corrupted LDM partition tables	MLIST	openwall.cor
oss-security - CVE request: kernel: fs/partitions: Kernel heap overflow via corrupted LDM partition tables	MLIST	openwall.cor
www.pre-cert.de/advisories/PRE-SA-2011-01.txt	MISC	www.pre-cer
oss-security - Re: CVE request: kernel: fs/partitions: Kernel heap overflow via corrupted LDM partition tables	MLIST	openwall.cor
Linux Kernel 'fs/partitions/ldm.c' Buffer Overflow and Denial of Service Vulnerabilities	BID	www.securit
Linux Kernel Buffer Overflow ldm_frag_add() Elevated Privileges - SecurityReason.com	SREASON	securityreas
Linux Kernel "ldm_frag_add()" Buffer Overflow Vulnerability - Secunia.com	SECUNIA	secunia.com
Linux Kernel "ldm_frag_add()" Buffer Overflow Vulnerability - Secunia.com	SECUNIA	secunia.com

SecurityFocus	BUGTRAQ	www.security
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.