CVE-2006-5466

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

Summary

CVE	CVE-2006-5466
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-11-06 17:07:00 UTC
Updated	2011-03-08 02:43:00 UTC
Description	Heap-based buffer overflow in the showQueryPackage function in librpm in RPM Package Manager 4.4.8, when the LANG

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rpm	Package Manager	4.4.8	All	All	All
Application	Rpm	Package Manager	4.4.8	All	All	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	All	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	i386	All
Operating System	Ubuntu	Ubuntu Linux	6.06_lts	All	All	All
Operating System	Ubuntu	Ubuntu Linux	6.10	All	i386	All

References

Reference	Source	Link
Bug 212833 – CVE-2006-5466 RPM Crash after listing contents of non-installed package	MISC	bugzilla.r
Advisories - Mandriva Linux	MANDRIVA	www.ma
Mandriva update for librpm4 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.c
RPM: Buffer overflow — Gentoo Linux Documentation	GENTOO	security.g
Gentoo update for librmp4 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.c
usn/usn-378-1 - Ubuntu: Linux for human beings	UBUNTU	www.ubu
Ubuntu update for librpm4 - Advisories - Secunia	SECUNIA	secunia.c
RPM Lets Remote Users Cause Arbitrary Code to Be Executed When Queried in Certain Locales - SecurityTracker	SECTRACK	securityt

LibRPM Query Report Arbitrary Code Execution Vulnerability	BID	www.sec
RPM Buffer Overflow Vulnerability - Advisories - Secunia	SECUNIA	secunia.c
Webmail - OVH	VUPEN	www.vup
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-03-14	Joshua Bressers	Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.c

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