CVE-2006-5753

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

Summary

CVE	CVE-2006-5753
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-01-30 19:28:00 UTC
Updated	2023-02-13 02:16:00 UTC
Description	Unspecified vulnerability in the listxattr system call in Linux kernel, when a "bad inode" is present, allows local users to caus

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.20.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.1	All	All	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora Core 6 Update: kernel-2.6.19-1.2911.6.4.fc6 | FedoraNEWS.ORG	FEDORA	fedoranews.org
306891 – (CVE-2006-5753) CVE-2006-5753 kernel listxattr syscall can corrupt user space programs	MISC	bugzilla.redhat.com
SUSE update for kernel - Advisories - Secunia	SECUNIA	secunia.com
usn/usn-416-1 - Ubuntu: Linux for human beings	UBUNTU	www.ubuntu.com

Mandriva update for kernel - Advisories - Secunia	SECUNIA	secunia.com
SUSE update for kernel - Advisories - Secunia	SECUNIA	secunia.com
rhn.redhat.com | Red Hat Support	REDHAT	www.redhat.com
rPath update for kernel - Advisories - Secunia	SECUNIA	secunia.com
Ubuntu update for kernel - Advisories - Secunia	SECUNIA	secunia.com
Linux Kernel "listxattr" Memory Corruption and Denial of Service - Advisories - Secunia	SECUNIA	secunia.com
Debian update for kernel-source-2.6.8 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
Security Announcement	SUSE	www.novell.com
Red Hat update for kernel - Advisories - Secunia	SECUNIA	secunia.com
Advisories | Mandriva	MANDRIVA	www.mandriva.com
rPath update for kernel and xen - Advisories - Secunia	SECUNIA	secunia.com
Security Announcement	SUSE	www.novell.com
Linux Kernel ListXATTR Local Denial of Service Vulnerability	BID	www.securityfocus.co
Repository / Oval Repository	OVAL	oval.cisecurity.org
Advisories - Mandriva Linux	MANDRIVA	www.mandriva.com
33020	OSVDB	osvdb.org
LKML: Eric Sandeen: [PATCH] fix memory corruption from misinterpreted bad_inode_ops return values	MISC	lkml.org
Fedora update for kernel - Secunia.com	SECUNIA	secunia.com
[SECURITY] Fedora Core 5 Update: kernel-2.6.19-1.2288.2.1.fc5 | FedoraNEWS.ORG	FEDORA	fedoranews.org
Security Announcement	SUSE	www.novell.com
Avaya Products Kernel Multiple Vulnerabilities - Advisories - Secunia	SECUNIA	secunia.com
Red Hat Customer Portal	MISC	access.redhat.com
Debian -- Security Information -- DSA-1503-1 kernel-source-2.4.27	DEBIAN	www.debian.org
SUSE update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
issues.rpath.com/browse/RPL-1106	CONFIRM	issues.rpath.com
SecurityFocus	BUGTRAQ	www.securityfocus.co
Debian -- Security Information -- DSA-1304-1 kernel-source-2.6.8	DEBIAN	www.debian.org
Security Announcement	SUSE	www.novell.com
Debian update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
Mandriva update for kernel - Advisories - Secunia	SECUNIA	secunia.com
access.redhat.com | CVE-2006-5753	MISC	access.redhat.com
ASA-2007-063 (RHSA-2007-0014)	CONFIRM	support.avaya.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credits

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-10-18	Mark J Cox	Red Hat Enterprise Linux 2.1 is not vulnerable to this issue as it only affects x86_64 architecture

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