



CVE-2007-4573

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

Summary

CVE	CVE-2007-4573
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-09-24 22:17:00 UTC
Updated	2018-10-15 21:36:00 UTC
Description	The IA32 system call emulation functionality in Linux kernel 2.4.x and 2.6.x before 2.6.22.7, when running on the x86_64 ar

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	x86_64	All
Operating System	Linux	Linux Kernel	All	All	x86_64	All

References

Reference	Source	Link	Tags
[SECURITY] Fedora Core 6 Update: kernel-2.6.22.7-57.fc6	FEDORA	www.redhat.com	
Red Hat update for kernel - Advisories - Secunia	SECUNIA	secunia.com	
LKML: Chris Wright: Re: Linux 2.6.22.7	MLIST	lkml.org	
'[Full-disclosure] COSEINC Linux Advisory #2: IA32 System Call' - MARC	FULLDISC	marc.info	
Security Announcement	SUSE	www.novell.com	
SUSE update for kernel - Advisories - Secunia	SECUNIA	secunia.com	
SecurityFocus	BUGTRAQ	www.securityfocus.com	
Linux Kernel Ptrace Local Privilege Escalation Vulnerability	BID	www.securityfocus.com	
rPath update for kernel - Advisories - Secunia	SECUNIA	secunia.com	
Debian update for kernel - Advisories - Secunia	SECUNIA	secunia.com	
Linux Kernel IA32 System Call Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTrack	securitytracker.com	
Linux Kernel ptrace Local Privilege Escalation Vulnerability - Advisories - Secunia	SECUNIA	secunia.com	

issues.rpath.com/browse/RPL-1754	CONFIRM	issues.rpath.com	
Debian -- Security Information -- DSA-1504-1 kernel-source-2.6.8	DEBIAN	www.debian.org	
SUSE update for kernel - Advisories - Secunia	SECUNIA	secunia.com	
rhn.redhat.com Red Hat Support	REDHAT	www.redhat.com	
Debian update for kernel - Advisories - Secunia	SECUNIA	secunia.com	
Repository / Oval Repository	OVAL	oval.cisecurity.org	
SecurityFocus	BUGTRAQ	www.securityfocus.com	
Support / Security / Advisories // MDVSA-2008:008 Mandriva	MANDRIVA	www.mandriva.com	
LKML: Chris Wright: Linux 2.6.22.7	MLIST	lkml.org	Patch
Support / Security / Advisories // MDKSA-2007:196 Mandriva	MANDRIVA	www.mandriva.com	
Support / Security / Advisories // MDKSA-2007:195 Mandriva	MANDRIVA	www.mandriva.com	
Fedora update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com	
404 Not Found	FEDORA	fedoranews.org	
Support / Security / Advisories // MDVSA-2008:105 Mandriva	MANDRIVA	www.mandriva.com	
rhn.redhat.com Red Hat Support	REDHAT	www.redhat.com	
404: File not found	CONFIRM	www.kernel.org	
rhn.redhat.com Red Hat Support	REDHAT	www.redhat.com	
404: File not found	CONFIRM	kernel.org	
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.opensuse.org	
Fedora update for kernel - Advisories - Secunia	SECUNIA	secunia.com	
Webmail - OVH	VUPEN	www.vupen.com	
Ubuntu update for kernel - Advisories - Secunia	SECUNIA	secunia.com	
Debian -- Security Information -- DSA-1378-2 linux-2.6	DEBIAN	www.debian.org	
Debian -- Security Information -- DSA-1381-2 linux-2.6	DEBIAN	www.debian.org	
USN-518-1: Linux kernel vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com	
Mandriva update for kernel - Advisories - Secunia	SECUNIA	secunia.com	
Debian update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni



Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-09-27	Mark J Cox	This issue affected users who were running 64-bit versions of Red Hat Enterprise Linux 3, 4, or 5.



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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)