



CVE-2005-3783

Published on: 11/23/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:23 PM UTC

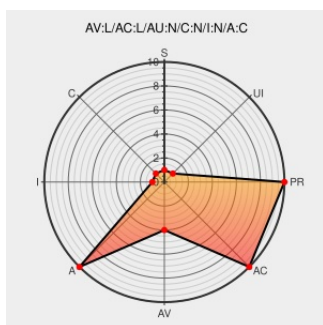
CVE-2005-3783

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

The ptrace functionality (ptrace.c) in Linux kernel 2.6 before 2.6.14.2, using CLONE_THREAD, does not use the thread group ID to check whether it is attaching to itself, which allows local users to cause a denial of service (crash).

CVE-2005-3783 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.9 - MEDIUM**

Access Vector

LOCAL

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

NONE

Availability Impact

COMPLETE

CVE References

Description

Tags

Link

Secunia - Advisories - Debian update for kernel-source-2.4.27

[web.archive.org](#)
[text/html](#)

[X](#) SECUNIA 19369

Advisories - Mandriva

[www.mandriva.com](#)
[text/html](#)

[MANDRIVA MDKSA-2006:072](#)

Linux Kernel PTrace CLONE_THREAD Local Denial of Service Vulnerability

[cve.report \(archive\)](#)
[text/html](#)

[BID 15642](#)

174075 – [RHEL4] CVE-2005-3783 ptrace DoS

[bugzilla.redhat.com](#)
[text/html](#)

[MISC bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174075](#)

SecurityFocus

[www.securityfocus.com](#)

[SUSE SUSE-SA:2005:068](#)

	text/html	
Advisory: kernel	web.archive.org text/html Inactive Link Not Archived	 SUSE SUSE-SA:2005:067
Advisories - Mandriva Linux	www.mandriva.com text/html	 MANDRIVA MDKSA-2006:018
404: File not found	www.kernel.org text/plain Inactive Link Not Archived	 CONFIRM www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.14.2
Debian update for kernel-source-2.6.8 - Advisories - Secunia	web.archive.org text/html	 SECUNIA 19374
No Description Provided	patches.sgi.com Inactive Link Not Archived	 SGI 20060402-01-U
No Description Provided	www.kernel.org text/html Inactive Link Not Archived	 CONFIRM www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.14.y.git;a=blobdiff;h=fcfc4568b45f3f190ba320b0d5853836921cb8bc;hp=019e04ec0f
Secunia - Advisories - Ubuntu update for kernel	web.archive.org text/html	 SECUNIA 18203
Debian -- Security Information -- DSA-1018-2 kernel-source-2.4.27	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1018
No Description Provided	www.kernel.org text/html Inactive Link Not Archived	 CONFIRM www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.14.y.git;a=commit;f
USN-231-1: Linux kernel vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-231-1
Secunia - Advisories - Fedora update for kernel	web.archive.org text/html	 SECUNIA 17787
Secunia - Advisories - SUSE update for kernel	web.archive.org text/html	 SECUNIA 17917
Secunia - Advisories - Linux Kernel ptrace Denial of Service Vulnerability	web.archive.org text/html	 SECUNIA 17761
Secunia - Advisories - SUSE update for kernel	web.archive.org text/html	 SECUNIA 17918
Debian -- Security Information -- DSA-1017-1 kernel-source-2.6.8	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1017
SGI ProPack kernel Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	 SECUNIA 19607

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.1	All	All	All

Operating System	Linux	Linux Kernel	2.6.12.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.14.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.8.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	All	All

Operating System	Linux	Linux Kernel	2.6.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc3	All	All

Operating System	Linux	Linux Kernel	2.6.14	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.14.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.8.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
cpe:2.3:o:linux:linux_kernel:2.6.0:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.1:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.10:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.1:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.10:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.11:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.12:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.2:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.3:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.4:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.5:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.6:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.7:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.8:*:*:*:*:*:						

cpe:2.3:o:linux:linux_kernel:2.6.11.9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14:rc2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14:rc3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14:rc4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.9:2.6.20:*****:
cpe:2.3:o:linux:linux_kernel:2.6.0:*****:
cpe:2.3:o:linux:linux_kernel:2.6.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.11:*****:

cpe:2.3:o:linux:linux_kernel:2.6.11.11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.12:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14:rc2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14:rc3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14:rc4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8:*****:

cpe:2.3:o:linux:linux_kernel:2.6.8.1:*****:

cpe:2.3:o:linux:linux_kernel:2.6.9:2.6.20:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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](#).

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