

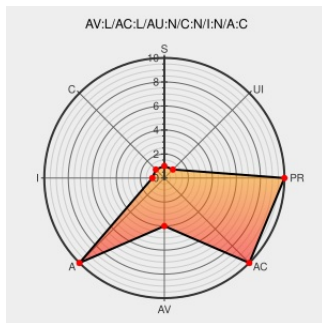


CVE-2005-3784

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

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-3784

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The auto-reap of child processes in Linux kernel 2.6 before 2.6.15 includes processes with ptrace attached, which leads to a dangling ptrace reference and allows local users to cause a denial of service (crash) and gain root privileges.

CVE-2005-3784 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

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[Vendor Advisory](#)
[www.vupen.com](#)
[text/html](#)

[VUPEN ADV-2005-2649](#)

kernel/git/torvalds/linux.git - Linux kernel source tree

[www.kernel.org](#)
[text/html](#)

[CONFIRM](#) [www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=7ed0175a462c4c30f6df6fac1cccac058f997739](#)

SecurityFocus

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

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

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](#)

Linux Kernel PTraced Child Auto-Reap Local Denial of Service Vulnerability	cve.report (archive) text/html	 BID 15625
Debian update for kernel-source-2.6.8 - Advisories - Secunia	Vendor Advisory web.archive.org text/html	 SECUNIA 19374
	www.trustix.org text/plain Inactive Link Not Archived	 TRUSTIX TSLSA-2005-0070
174078 – [RHEL4] CVE-2005-3784 auto-reap DoS	bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174078
Secunia - Advisories - Ubuntu update for kernel	Vendor Advisory web.archive.org text/html	 SECUNIA 18203
Secunia - Advisories - Red Hat update for kernel	Vendor Advisory web.archive.org text/html	 SECUNIA 18510
SecurityFocus	www.securityfocus.com text/html	 FEDORA FLSA:157459-4
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:9080
Secunia - Advisories - Linux Kernel Multiple Denial of Service Vulnerabilities	Vendor Advisory web.archive.org text/html	 SECUNIA 17786
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	Vendor Advisory web.archive.org text/html	 SECUNIA 17917
Secunia - Advisories - SUSE update for kernel	Vendor Advisory 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
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20060706 Re: [MDKSA-2006:116] - Updated kernel packages fixes multiple vulnerabilities
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2006:0101

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	2.6.12.2	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	2.6.12.5	All	All	All

Operating System	Linux	Linux Kernel	2.6.12.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.7	All	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	2.6.11.1	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	2.6.12.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.1	All	All	All

Operating System	Linux	Linux Kernel	2.6.14.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.7	All	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:2.6.12.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.7:*****:
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:2.6.11.6:*****:
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:2.6.12.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.14.7:*****:

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](#)