



CVE-2005-3805

Published on: 11/25/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

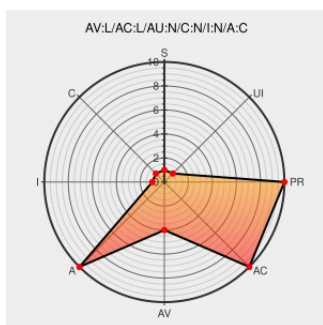
CVE-2005-3805

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

A locking problem in POSIX timer cleanup handling on exit in Linux kernel 2.6.10 to 2.6.14, when running on SMP systems, allows local users to cause a denial of service (deadlock) involving process CPU timers.

CVE-2005-3805 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

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

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

[CONFIRM kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=25f407f0b668f5e4ebd5d13e1fb4306ba6427ead](#)

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 POSIX Timer Cleanup Handling Local Denial of Service Vulnerability

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

[BID 15722](#)

Secunia - Advisories - Ubuntu update for kernel	web.archive.org text/html	 SECUNIA 18203
SecurityFocus	www.securityfocus.com text/html	 FEDORA FLSA:157459-4
USN-231-1: Linux kernel vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-231-1
Secunia - Advisories - SUSE update for kernel	web.archive.org text/html	 SECUNIA 17917
Secunia - Advisories - SUSE update for kernel	web.archive.org text/html	 SECUNIA 17918

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	2.6.10	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

System						
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	2.6.10	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

System						
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
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:2.6.11.0:*****:
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:2.6.10:*****:
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:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)