



CVE-2005-1913

Published on: 09/14/2005 12:00:00 AM UTC

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

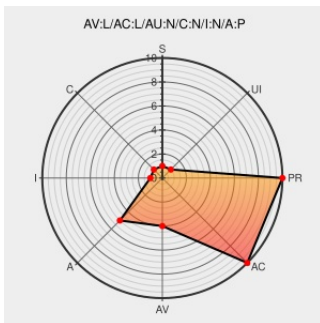
CVE-2005-1913

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The Linux kernel 2.6 before 2.6.12.1 allows local users to cause a denial of service (kernel panic) via a non group-leader thread executing a different program than was pending in itimer, which causes the signal to be delivered to the old group-leader task, which does not exist.

CVE-2005-1913 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **2.1 - LOW**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Secunia - Advisories - Linux Kernel Multiple Vulnerabilities

Patch
Vendor Advisory
web.archive.org
text/html

SECUNIA 15786

Linux Kernel Subthread Exec Local Denial Of Service Vulnerability

Patch
cve.report (archive)
text/html

BID 14054

usn/usn-178-1 - Ubuntu Linux

www.ubuntu.com
text/html

UBUNTU USN-178-1

IBM X-Force Exchange

exchange.xforce.ibmcloud.com
text/html

XF kernel-subthread-dos(21138)

kernel.org
text/plain

CONFIRM
kernel.org/pub/linux/kernel/v2.6/ChangeLog-

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	2.6.0	test1	All	All
Operating System	Linux	Linux Kernel	2.6.0	test10	All	All
Operating System	Linux	Linux Kernel	2.6.0	test11	All	All
Operating System	Linux	Linux Kernel	2.6.0	test2	All	All
Operating System	Linux	Linux Kernel	2.6.0	test3	All	All
Operating System	Linux	Linux Kernel	2.6.0	test4	All	All
Operating System	Linux	Linux Kernel	2.6.0	test5	All	All
Operating System	Linux	Linux Kernel	2.6.0	test6	All	All
Operating System	Linux	Linux Kernel	2.6.0	test7	All	All
Operating System	Linux	Linux Kernel	2.6.0	test8	All	All
Operating System	Linux	Linux Kernel	2.6.0	test9	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	rc2	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	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.11.11	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	2.6.12	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc4	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	2.6.6	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc4	All	All

Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
Operating System	Linux	Linux Kernel	2.6_test9_cvs	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	test1	All	All
Operating System	Linux	Linux Kernel	2.6.0	test10	All	All
Operating System	Linux	Linux Kernel	2.6.0	test11	All	All
Operating System	Linux	Linux Kernel	2.6.0	test2	All	All
Operating System	Linux	Linux Kernel	2.6.0	test3	All	All
Operating System	Linux	Linux Kernel	2.6.0	test4	All	All
Operating System	Linux	Linux Kernel	2.6.0	test5	All	All
Operating System	Linux	Linux Kernel	2.6.0	test6	All	All
Operating System	Linux	Linux Kernel	2.6.0	test7	All	All
Operating System	Linux	Linux Kernel	2.6.0	test8	All	All
Operating System	Linux	Linux Kernel	2.6.0	test9	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc4	All	All

Operating System	Linux	Linux Kernel	2.6.11.11	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	2.6.12	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc4	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	2.6.6	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
Operating System	Linux	Linux Kernel	2.6_test9_cvs	All	All	All
cpe:2.3:o:linux:linux_kernel:2.6.0:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.0:test1:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.0:test10:*:*:*:*:*:						

cpe:2.3:o:linux:linux_kernel:2.6.0:test1:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.0:test2:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.0:test3:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.0:test4:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.0:test5:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.0:test6:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.0:test7:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.0:test8:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.0:test9:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.1:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.1:rc1:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.1:rc2:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.10:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.10:rc2:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.11:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.11:rc2:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.11:rc3:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.11:rc4:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.11.11:*****:*
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:2.6.12:rc1:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.12:rc4:*****:*
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:2.6.6:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.7:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8:rc2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8:rc3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.9:2.6.20:*****:
cpe:2.3:o:linux:linux_kernel:2.6_test9_cvs:*****:
cpe:2.3:o:linux:linux_kernel:2.6.0:*****:
cpe:2.3:o:linux:linux_kernel:2.6.0:test1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.0:test10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.0:test11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.0:test2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.0:test3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.0:test4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.0:test5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.0:test6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.0:test7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.0:test8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.0:test9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.1:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.1:rc2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.10:rc2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11:*****:

cpe:2.3:o:linux:linux_kernel:2.6.11:rc1:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc2:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc3:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc4:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.11:****:*:
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:2.6.12:rc1:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.12:rc4:****:*:
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:2.6.6:rc1:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.7:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.7:rc1:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.8:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.8:rc1:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.8:rc2:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.8:rc3:****:*:
cpe:2.3:o:linux:linux_kernel:2.6.9:2.6.20:****:*:
cpe:2.3:o:linux:linux_kernel:2.6_test9_cvs:****:*:

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](#)