



CVE-2005-2492

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

Last Modified on: 02/13/2023 01:09:26 AM UTC

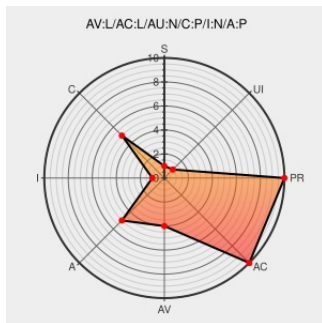
CVE-2005-2492

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The raw_sendmsg function in the Linux kernel 2.6 before 2.6.13.1 allows local users to cause a denial of service (change hardware state) or read from arbitrary memory via crafted input.

CVE-2005-2492 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **3.6 - LOW**

Access Vector

Access Complexity

Authentication

LOCAL

LOW

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

NONE

PARTIAL

CVE References

Description

Tags

Link

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

[CONFIRM](#)
www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13.1

SecurityFocus

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

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

Linux Kernel Raw_sendmsg() Kernel Memory Access Vulnerability

[Third Party Advisory](#)
[VDB Entry](#)
[cve.report \(archive\)](#)
[text/html](#)

[BID 14787](#)

Advisories - Mandriva Linux

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

[MANDRIVA MDKSA-2005:235](#)

SecurityFocus

www.securityfocus.com

[FEDORA FLSA:157459-3](#)

	text/html	
rhn.redhat.com Red Hat Support	Not Applicable www.redhat.com text/html	 REDHAT RHSA-2005:514
Secunia - Advisories - Linux Kernel Multiple Vulnerabilities	Permissions Required Third Party Advisory web.archive.org text/html	 SECUNIA 16747
Secunia - Advisories - Red Hat update for kernel	Permissions Required Third Party Advisory web.archive.org text/html	 SECUNIA 17073
'TSLSA-2005-0049 - multi' - MARC	Mailing List marc.info text/html	 TRUSTIX 2005-0049
usn/usn-178-1 - Ubuntu Linux	Third Party Advisory www.ubuntu.com text/html	 UBUNTU USN-178-1
Advisories - Mandriva Linux	www.mandriva.com text/html	 MANDRAKE MDKSA-2005:220
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF kernel-rawsendmsg-obtain-information(22218)
Secunia - Advisories - SUSE update for kernel	Permissions Required Third Party Advisory web.archive.org text/html	 SECUNIA 17918
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:11031
Bug 166830 – CAN-2005-2492 sendmsg DoS	Issue Tracking Patch bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/bugzilla/show_bug.cgi?id=166830

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	Canonical	Ubuntu Linux	4.10	All	All	All
Operating System	Canonical	Ubuntu Linux	5.04	All	All	All
Operating System	Canonical	Ubuntu Linux	4.10	All	All	All
Operating	Canonical	Ubuntu Linux	5.04	All	All	All

System						
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	2.6.11.6	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
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	test1	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	test1	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
Operating System	Redhat	Enterprise Linux	4.0	All	All	All
Operating System	Redhat	Enterprise Linux	4.0	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:4.10:*****:						
cpe:2.3:o:canonical:ubuntu_linux:5.04:*****:						
cpe:2.3:o:canonical:ubuntu_linux:4.10:*****:						
cpe:2.3:o:canonical:ubuntu_linux:5.04:*****:						
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: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: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:redhat:enterprise_linux:4.0:****:*:

cpe:2.3:o:redhat:enterprise_linux:4.0:****:*:

No vendor comments have been submitted for this CVE

© [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](#)