



CVE-2005-2973

Published on: 10/27/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:15:00 AM UTC

CVE-2005-2973

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

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

The `udp_v6_get_port` function in `udp.c` in Linux 2.6 before 2.6.14-rc5, when running IPv6, allows local users to cause a denial of service (infinite loop and crash).

CVE-2005-2973 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 - Debian update for kernel-source-2.4.27

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

SECUNIA 19369

Advisories - Mandriva

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

MANDRIVA MDKSA-2006:072

No Description Provided

[www.osvdb.org](#)

OSVDB 20163

Inactive Link Not Archived

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

Secunia - Advisories - Red Hat update for kernel	web.archive.org text/html	 SECUNIA 18562
SecurityFocus	www.securityfocus.com text/html	 FEDORA FLSA:157459-1
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2006:0190
170772 – CVE-2005-2973 ipv6 infinite loop	bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/bugzilla/show_bug.cgi?id=170772
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:10041
Red Hat update for kernel - Advisories - Secunia	web.archive.org text/html	 SECUNIA 20237
Avaya Products Linux Kernel Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	 SECUNIA 21745
Secunia - Advisories - SmoothWall Express Update for Multiple Packages	web.archive.org text/html	 SECUNIA 19185
No Description Provided	linux.bkbits.net Inactive Link Not Archived	 MISC linux.bkbits.net:8080/linux-2.6/cset%404342df67SNhRx_3FGhUrrU-FXLIQIA
Debian update for kernel-source-2.6.8 - Advisories - Secunia	web.archive.org text/html	 SECUNIA 19374
SecurityFocus	www.securityfocus.com text/html	 FEDORA FLSA:157459-3
Secunia - Advisories - Fedora update for kernel	web.archive.org text/html	 SECUNIA 17280
USN-219-1: Linux kernel vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-219-1
Advisory: Fedora Core 4 Update: kernel-2.6.13-1.1532_FC4	web.archive.org text/html Inactive Link Not Archived	 FEDORA FEDORA-2005-1013
Linux Kernel IPV6 Local Denial of Service Vulnerability	cve.report (archive) text/html	 BID 15156
Debian -- Security Information -- DSA-1018-2 kernel-source-2.4.27	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1018
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2006:0493
Secunia - Advisories - Linux Kernel IPv6 Denial of Service Vulnerability	web.archive.org text/html	 SECUNIA 17261
Advisories - Mandriva Linux	www.mandriva.com text/html	 MANDRIVA MDKSA-2006:040
Advisory: Fedora Core 3 Update: kernel-2.6.12-1.1380_FC3	web.archive.org text/html Inactive Link Not Archived	 FEDORA FEDORA-2005-1007
Secunia - Advisories - SUSE update for kernel	web.archive.org text/html	 SECUNIA 17917
ASA-2006-161 (RHSA-2006-0493)	support.avaya.com text/html	 CONFIRM support.avaya.com/slmodge2/security/ASA-2006

	text/html	support.avaya.com/en/10000652/Security/ASA-2000-161.htm
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
Webmail - OVH	www.vupen.com text/html	 VUPEN ADV-2005-2173
Secunia - Advisories - Red Hat update for kernel	web.archive.org text/html	 SECUNIA 18684
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2006:0191
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2006:0140
SecurityFocus	www.securityfocus.com text/html	 FEDORA FLSA:157459-2

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	2.6.13	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	2.6.2	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	2.6.11.1	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 Svsstem	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	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	2.6.2	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: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:2.6.2:****:*:*:
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:2.6.11.12:****:*:*:
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: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:2.6.2:****:*:*:
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→