



# CVE-2005-0736

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2005-0736
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-03-09 05:00:00 UTC
<b>Updated</b>	2023-11-07 01:57:00 UTC
<b>Description</b>	Integer overflow in sys_epoll_wait in eventpoll.c for Linux kernel 2.6 to 2.6.11 allows local users to overwrite kernel memory

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	10.0	All	All	All
Operating System	<a href="#">Conectiva</a>	<a href="#">Linux</a>	10.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.1	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.10	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.11	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.2	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.3	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.4	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.5	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.6	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.7	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.8	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.9	2.6.20	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.1	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.10	All	All	All

Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.11	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.2	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.3	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.4	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.5	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.6	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.7	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.8	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.9	2.6.20	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	advanced_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	enterprise_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	workstation	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	advanced_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	enterprise_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	workstation	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Fedora Core</a>	core_2.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Fedora Core</a>	core_3.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Fedora Core</a>	core_2.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Fedora Core</a>	core_3.0	All	All	All

## References

Reference	Source	Link	Tags
<a href="#">rhn.redhat.com   Red Hat Support</a>	REDHAT	<a href="#">www.redhat.com</a>	
<a href="#">Linux Kernel SYS_EPoll_Wait Local Integer Overflow Vulnerability</a>	BID	<a href="#">www.securityfocus.com</a>	Exploit, Patch, Vendor Advis
<a href="#">[Full-disclosure] overwriting low kernel memory</a>	FULLDISC	<a href="#">lists.grok.org.uk</a>	Patch, Vendor Advisory
<a href="#">Security Announcement</a>	SUSE	<a href="#">www.novell.com</a>	Vendor Advisory
<a href="#">Repository / Oval Repository</a>	OVAL	<a href="#">oval.cisecurity.org</a>	
<a href="#">USN-95-1: Linux kernel vulnerabilities   Ubuntu security notices</a>	UBUNTU	<a href="#">usn.ubuntu.com</a>	
<a href="#">rhn.redhat.com   Red Hat Support</a>	REDHAT	<a href="#">www.redhat.com</a>	
<a href="#">linux.bkbits.net/linux-2.6/cset%40422dd06a1p5PsyFhoGAJseinjEq3ew</a>		<a href="#">linux.bkbits.net</a>	
<a href="#">linux.bkbits.net/linux-2.6/cset@422dd06a1p5PsyFhoGAJseinjEq3ew</a>	CONFIRM	<a href="#">linux.bkbits.net</a>	Broken Link
<a href="#">CVE Program record</a>	CVE.ORG	<a href="#">www.cve.org</a>	canonical
<a href="#">NVD vulnerability detail</a>	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)**