CVE-2005-0736

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2005-0736
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-03-09 05:00:00 UTC
Updated	2023-11-07 01:57:00 UTC
Description	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	Conectiva	Linux	10.0	All	All	All
Operating System	Conectiva	Linux	10.0	All	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	2.6.2	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	2.6.9	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	2.6.2	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	2.6.9	2.6.20	All	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Redhat	Fedora Core	core_2.0	All	All	All
Operating System	Redhat	Fedora Core	core_3.0	All	All	All
Operating System	Redhat	Fedora Core	core_2.0	All	All	All
Operating System	Redhat	Fedora Core	core_3.0	All	All	All

References

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

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report