CVE-2010-4248

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2010-4248
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-11-30 21:38:00 UTC
Updated	2023-02-13 04:28:00 UTC
Description	Race condition in the __exit_signal function in kernel/exit.c in the Linux kernel before 2.6.37-rc2 allows local users to cause

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	2.6.37	-	All	All
Operating System	Linux	Linux Kernel	2.6.37	rc1	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	2.6.37	-	All	All
Operating System	Linux	Linux Kernel	2.6.37	rc1	All	All

References

Reference	Source	Li
oss-security - CVE request: kernel: posix-cpu-timers: workaround to suppress the problems with mt exec	MLIST	ww
404: File not found	CONFIRM	ww
Support	REDHAT	ww
SecurityFocus	BUGTRAQ	ww
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git
oss-security - Re: CVE request: kernel: posix-cpu-timers: workaround to suppress the problems with mt exec	MLIST	ww
Linux Kernel 'posix-cpu-timers.c' Local Race Condition Vulnerability	BID	ww
656264 – (CVE-2010-4248) CVE-2010-4248 kernel: posix-cpu-timers: workaround to suppress the problems with mt exec	CONFIRM	bu

mandriva.com	MANDRIVA	wv
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git
VMSA-2011-0012.2	CONFIRM	wv
Red Hat update for kernel - Advisories - Community	SECUNIA	se
About Secunia Research | Flexera	SECUNIA	se
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	wv
Red Hat update for kernel - Secunia.com	SECUNIA	se
access.redhat.com	REDHAT	wv
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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