CVE-2006-5755

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

Summary

CVE	CVE-2006-5755
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-12-31 05:00:00 UTC
Updated	2023-02-13 02:16:00 UTC
Description	Linux kernel before 2.6.18, when running on x86_64 systems, does not properly save or restore EFLAGS during a context s

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Advisories | Mandriva	MANDRIVA	www.mandriva.com	
Repository / Oval Repository	OVAL	oval.cisecurity.org	
usn/usn-416-1 - Ubuntu: Linux for human beings	UBUNTU	www.ubuntu.com	
404: File not found	CONFIRM	www.kernel.org	
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	kernel.org	
Red hat update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	kernel.org	
Ubuntu update for kernel - Advisories - Secunia	SECUNIA	secunia.com	
Linux Kernel EFLAGS NT Local Denial of Service Vulnerability	BID	www.securityfocus.com	
Debian update for kernel - Advisories - Secunia	SECUNIA	secunia.com	
rPath update for kernel and xen - Advisories - Secunia	SECUNIA	secunia.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	

Support	REDHAT	www.redhat.com	
404: File not found	CONFIRM	www.kernel.org	
SecurityFocus	BUGTRAQ	www.securityfocus.com	
Debian -- Security Information -- DSA-1381-2 linux-2.6	DEBIAN	www.debian.org	
Mandriva update for kernel - Advisories - Secunia	SECUNIA	secunia.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

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**