CVE-2007-5001

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

Summary

CVE	CVE-2007-5001
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-05-08 00:20:00 UTC
Updated	2017-09-29 01:29:00 UTC
Description	Linux kernel before 2.4.21 allows local users to cause a denial of service (kernel panic) via asynchronous input or output or

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	as_3	All	All	All
Operating System	Redhat	Enterprise Linux	es_3	All	All	All
Operating System	Redhat	Enterprise Linux	ws_3	All	All	All
Operating System	Redhat	Enterprise Linux	as_3	All	All	All
Operating System	Redhat	Enterprise Linux	es_3	All	All	All
Operating System	Redhat	Enterprise Linux	ws_3	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All

References

Reference	Source	Link
Linux Kernel Asynchronous FIFO IO Local Denial of Service Vulnerability	BID	www.security
Repository / Oval Repository	OVAL	oval.cisecuri
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.c
VMware ESX Server update for Samba and vmnix - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
IBM X-Force Exchange	XF	exchange.xfo
44987	OSVDB	osvdb.org

[Security-announce] VMSA-2008-00011 Updated ESX service console packages for Samba and vmnix	MLIST	lists.vmware
rhn.redhat.com | Red Hat Support	REDHAT	www.redhat.
Bug 326251 – CVE-2007-5001 kernel asynchronous IO on a FIFO kernel panic	CONFIRM	bugzilla.redh
Red Hat update for kernel - Advisories - Secunia	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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**