CVE-2004-0554

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2004-0554
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-08-06 04:00:00 UTC
Updated	2017-10-11 01:29:00 UTC
Description	Linux kernel 2.4.x and 2.6.x for x86 allows local users to cause a denial of service (system crash), possibly via an infinite lo

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Avaya	Converged Communications Server	2.0	All	All	All
Hardware	Avaya	Converged Communications Server	2.0	All	All	All
Application	Avaya	Intuity Audix	All	All	lx	All
Application	Avaya	Intuity Audix	All	All	lx	All
Operating System	Avaya	Modular Messaging Message Storage Server	s3400	All	All	All
Operating System	Avaya	Modular Messaging Message Storage Server	s3400	All	All	All
Hardware	Avaya	S8300	r2.0.0	All	All	All
Hardware	Avaya	S8300	r2.0.1	All	All	All
Hardware	Avaya	S8300	r2.0.0	All	All	All
Hardware	Avaya	S8300	r2.0.1	All	All	All
Hardware	Avaya	S8500	r2.0.0	All	All	All
Hardware	Avaya	S8500	r2.0.1	All	All	All
Hardware	Avaya	S8500	r2.0.0	All	All	All
Hardware	Avaya	S8500	r2.0.1	All	All	All
Hardware	Avaya	S8700	r2.0.0	All	All	All
Hardware	Avaya	S8700	r2.0.1	All	All	All
Hardware	Avaya	S8700	r2.0.0	All	All	All

Hardware	Avaya	S8700	r2.0.1	All	All	All
Operating System	Conectiva	Linux	8.0	All	All	All
Operating System	Conectiva	Linux	9.0	All	All	All
Operating System	Conectiva	Linux	8.0	All	All	All
Operating System	Conectiva	Linux	9.0	All	All	All
Operating System	Gentoo	Linux	1.4	All	All	All
Operating System	Gentoo	Linux	1.4	All	All	All
Operating System	Linux	Linux Kernel	2.4.18	All	All	All
Operating System	Linux	Linux Kernel	2.4.19	All	All	All
Operating System	Linux	Linux Kernel	2.4.21	All	All	All
Operating System	Linux	Linux Kernel	2.4.22	All	All	All
Operating System	Linux	Linux Kernel	2.4.23	All	All	All
Operating System	Linux	Linux Kernel	2.4.24	All	All	All
Operating System	Linux	Linux Kernel	2.4.25	All	All	All
Operating System	Linux	Linux Kernel	2.4.26	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	2.6.1	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc2	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	2.6.6	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	rc1	All	All
Operating System	Linux	Linux Kernel	2.4.18	All	All	All
Operating System	Linux	Linux Kernel	2.4.19	All	All	All
Operating System	Linux	Linux Kernel	2.4.21	All	All	All
Operating System	Linux	Linux Kernel	2.4.22	All	All	All
Operating System	Linux	Linux Kernel	2.4.23	All	All	All
Operating System	Linux	Linux Kernel	2.4.24	All	All	All
Operating System	Linux	Linux Kernel	2.4.25	All	All	All
Operating System	Linux	Linux Kernel	2.4.26	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	2.6.1	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc2	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	2.6.6	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	rc1	All	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_servers	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_servers	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation	All
Application	Suse	Suse Email Server	3.1	All	All	All
Application	Suse	Suse Email Server	iii	All	All	All
Application	Suse	Suse Email Server	3.1	All	All	All
Application	Suse	Suse Email Server	iii	All	All	All
Operating System	Suse	Suse Linux	7	All	enterprise_server	All
Operating System	Suse	Suse Linux	8	All	enterprise_server	All
Operating System	Suse	Suse Linux	8.0	All	All	All
Operating System	Suse	Suse Linux	8.0	All	i386	All
Operating System	Suse	Suse Linux	8.1	All	All	All
Operating System	Suse	Suse Linux	8.2	All	All	All
Operating System	Suse	Suse Linux	9.0	All	All	All

Operating System	Suse	Suse Linux	9.0	All	x86_64	All
Operating System	Suse	Suse Linux	9.1	All	All	All
Operating System	Suse	Suse Linux	7	All	enterprise_server	All
Operating System	Suse	Suse Linux	8	All	enterprise_server	All
Operating System	Suse	Suse Linux	8.0	All	All	All
Operating System	Suse	Suse Linux	8.0	All	i386	All
Operating System	Suse	Suse Linux	8.1	All	All	All
Operating System	Suse	Suse Linux	8.2	All	All	All
Operating System	Suse	Suse Linux	9.0	All	All	All
Operating System	Suse	Suse Linux	9.0	All	x86_64	All
Operating System	Suse	Suse Linux	9.1	All	All	All
Application	Suse	Suse Linux Admin-cd For Firewall	All	All	All	All
Application	Suse	Suse Linux Admin-cd For Firewall	All	All	All	All
Application	Suse	Suse Linux Connectivity Server	All	All	All	All
Application	Suse	Suse Linux Connectivity Server	All	All	All	All
Application	Suse	Suse Linux Database Server	All	All	All	All
Application	Suse	Suse Linux Database Server	All	All	All	All
Application	Suse	Suse Linux Firewall Cd	All	All	All	All
Application	Suse	Suse Linux Firewall Cd	All	All	All	All
Application	Suse	Suse Linux Office Server	All	All	All	All
Application	Suse	Suse Linux Office Server	All	All	All	All
Application	Suse	Suse Office Server	All	All	All	All
Application	Suse	Suse Office Server	All	All	All	All

References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-1067-1 kernel-source-2.4.16	DEBIAN	www.debian.org	
2004-0034	TRUSTIX	www.trustix.net	
Gentoo Linux Documentation -- Linux Kernel: Multiple vulnerabilities	GENTOO	security.gentoo.org	
Debian -- Security Information -- DSA-1070-1 kernel-source-2.4.19	DEBIAN	www.debian.org	
Linux Kernel Floating Point Exception Handler Local Denial Of Service Vulnerability	BID	www.securityfocus.com	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
'timer + fpu stuff locks my console race' - MARC	MLIST	marc.info	
sources.redhat.com	MISC	gcc.gnu.org	
Debian -- Security Information -- DSA-1082-1 kernel-source-2.4.17	DEBIAN	www.debian.org	
Secunia - Advisories - Debian update for kernel-source-2.4.16	SECUNIA	secunia.com	

US-CERT Vulnerability Note VU#973654	CERT-VN	www.kb.cert.org	Third
Repository / Oval Repository	OVAL	oval.cisecurity.org	
Secunia - Advisories - Debian update for kernel-source-2.4.18	SECUNIA	secunia.com	
Repository / Oval Repository	OVAL	oval.cisecurity.org	
404 Page Not Found | SUSE	SUSE	www.novell.com	
LWN: Fedora alert FEDORA-2004-186 (kernel)	FEDORA	lwn.net	
June 11th, 2004: New Kernel Crash-Exploit discovered - LinuxReviews	MISC	linuxreviews.org	
redhat.com | Red Hat Support	REDHAT	www.redhat.com	
Secunia - Advisories - Debian update for kernel-source-2.4.17	SECUNIA	secunia.com	
'[ESA-20040621-005] 'kernel' Several vulnerabilities' - MARC	ENGARDE	marc.info	
20040620 TSSA-2004-011 - kernel	BUGTRAQ	marc.info	
Advisories - Mandriva	MANDRAKE	www.mandriva.com	
Debian -- Security Information -- DSA-1069-1 kernel-source-2.4.18	DEBIAN	www.debian.org	
Secunia - Advisories - Debian update for kernel-source-2.4.19	SECUNIA	secunia.com	
Home - Conectiva	CONECTIVA	distro.conectiva.com.br	
redhat.com | Red Hat Support	REDHAT	www.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

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