CVE-2009-2848

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2009-2848
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-08-18 21:00:00 UTC
Updated	2020-08-28 13:10:00 UTC
Description	The execve function in the Linux kernel, possibly 2.6.30-rc6 and earlier, does not properly clear the current->clear_child_tid

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Fedoraproject	Fedora	11	All	All	All
Operating System	Fedoraproject	Fedora	11	All	All	All
Operating System	Linux	Linux Kernel	2.6.30	-	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc6	All	All

Operating System	Linux	Linux Kernel	2.6.30	-	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.30	rc6	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Novell	Linux Desktop	9	All	All	All
Operating System	Novell	Linux Desktop	9	All	All	All
Operating System	Opensuse	Opensuse	11.0	All	All	All
Operating System	Opensuse	Opensuse	11.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp2	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp2	All	All
Operating System	Suse	Linux Enterprise Server	10	sp2	All	All
Operating System	Suse	Linux Enterprise Server	9	All	All	All
Operating System	Suse	Linux Enterprise Server	10	sp2	All	All
Operating System	Suse	Linux Enterprise Server	9	All	All	All
Operating System	Vmware	Esx	4.0	All	All	All
Operating System	Vmware	Esx	4.0	All	All	All
Application	Vmware	Vma	4.0	All	All	All

Application	Vmware	Vma		4.0	All	All	All

References

Reference	Source	Link
oss-security - CVE request - kernel: execve: must clear current->clear_child_tid	MLIST	www.ope
Support	REDHAT	www.redh
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.open
rhn.redhat.com | Red Hat Support	REDHAT	rhn.redha
Red Hat update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.c
Gmane -- Mail To News And Back Again	MLIST	article.gm
SecurityFocus	BUGTRAQ	www.secu
Linux Kernel "clear_child_tid" Memory Corruption - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.c
Repository / Oval Repository	OVAL	oval.cisec
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vup
IBM X-Force Exchange	XF	exchange
oss-security - Re: CVE request - kernel: execve: must clear current->clear_child_tid	MLIST	www.ope
Ubuntu update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.c
SUSE update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.c
[SECURITY] Fedora 11 Update: kernel-2.6.29.6-217.2.16.fc11	FEDORA	www.redh
Red Hat update for kernel - Secunia.com	SECUNIA	secunia.c
Repository / Oval Repository	OVAL	oval.cisec
Repository / Oval Repository	OVAL	oval.cisec
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.open
USN-852-1: Linux kernel vulnerabilities | Ubuntu	UBUNTU	www.ubu
SecurityFocus	BUGTRAQ	www.secu
VMSA-2009-0016.1	CONFIRM	www.vmv
rhn.redhat.com | Red Hat Support	REDHAT	rhn.redha
Fedora update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.c
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	lists.open
VMware ESX and vMA Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.c
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

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