



# CVE-2009-2848

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2009-2848
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-08-18 21:00:00 UTC
<b>Updated</b>	2020-08-28 13:10:00 UTC
<b>Description</b>	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	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	6.06	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	8.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	8.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	9.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	6.06	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	8.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	8.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	9.04	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	11	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	11	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.30	-	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.30	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.30	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.30	rc3	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.30	rc4	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	2.6.30	rc5	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	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	<a href="http://www.ope">www.ope</a>
Support	REDHAT	<a href="http://www.redh">www.redh</a>
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	<a href="http://lists.open">lists.open</a>
<a href="http://rhn.redhat.com">rhn.redhat.com</a>   Red Hat Support	REDHAT	<a href="http://rhn.redha">rhn.redha</a>
Red Hat update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	<a href="http://secunia.c">secunia.c</a>
Gmane -- Mail To News And Back Again	MLIST	<a href="http://article.gr">article.gr</a>
SecurityFocus	BUGTRAQ	<a href="http://www.seci">www.seci</a>
Linux Kernel "clear_child_tid" Memory Corruption - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	<a href="http://secunia.c">secunia.c</a>
Repository / Oval Repository	OVAL	<a href="http://oval.cisec">oval.cisec</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupr">www.vupr</a>
IBM X-Force Exchange	XF	<a href="http://exchange">exchange</a>
oss-security - Re: CVE request - kernel: execve: must clear current->clear_child_tid	MLIST	<a href="http://www.ope">www.ope</a>
Ubuntu update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	<a href="http://secunia.c">secunia.c</a>
SUSE update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	<a href="http://secunia.c">secunia.c</a>
[SECURITY] Fedora 11 Update: kernel-2.6.29.6-217.2.16.fc11	FEDORA	<a href="http://www.redh">www.redh</a>
Red Hat update for kernel - Secunia.com	SECUNIA	<a href="http://secunia.c">secunia.c</a>
Repository / Oval Repository	OVAL	<a href="http://oval.cisec">oval.cisec</a>
Repository / Oval Repository	OVAL	<a href="http://oval.cisec">oval.cisec</a>
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	<a href="http://lists.open">lists.open</a>
USN-852-1: Linux kernel vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubu">www.ubu</a>
SecurityFocus	BUGTRAQ	<a href="http://www.seci">www.seci</a>
VMSA-2009-0016.1	CONFIRM	<a href="http://www.vmv">www.vmv</a>
<a href="http://rhn.redhat.com">rhn.redhat.com</a>   Red Hat Support	REDHAT	<a href="http://rhn.redha">rhn.redha</a>
Fedora update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	<a href="http://secunia.c">secunia.c</a>
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	SUSE	<a href="http://lists.open">lists.open</a>
VMware ESX and vMA Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	<a href="http://secunia.c">secunia.c</a>
CVE Program record	CVE.ORG	<a href="http://www.cve">www.cve</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.g">nvd.nist.g</a>

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**