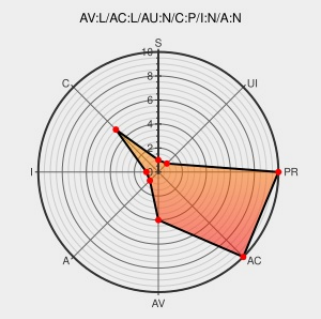
CVE-2009-3228

Published on: 10/19/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:25 PM UTC

CVE-2009-3228

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The tc_fill_tclass function in net/sched/sch_api.c in the tc subsystem in the Linux kernel 2.4.x before 2.4.37.6 and 2.6.x before 2.6.31-rc9 does not initialize certain (1) tcm__pad1 and (2) tcm__pad2 structure members, which might allow local users to obtain sensitive information from kernel memory via unspecified vectors.

CVE-2009-3228 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
oss-security - Re: CVE request: kernel: tc: uninitialised kernel memory leak	Mailing List, Patch, Third Party Advisory, www.openwall.com, text/html	MLIST [oss-security] 20090917 Re: CVE request: kernel: tc: uninitialised kernel memory leak
oss-security - CVE request: kernel: tc: uninitialised kernel memory leak	Mailing List, Patch, Third Party Advisory, www.openwall.com, text/html	MLIST [oss-security] 20090903 CVE request: kernel: tc: uninitialised kernel memory leak
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch, Vendor Advisory, git.kernel.org	CONFIRM git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=16ebb5e0b36ceadc8186f71d68b0c4fa4b6e781b

	text/html	
Red Hat update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	Third Party Advisory web.archive.org text/html	SECUNIA 37084
Repository / Oval Repository	Third Party Advisory oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:6757
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	VUPEN ADV-2010-0528
oss-security - Re: CVE request: kernel: tc: uninitialised kernel memory leak	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20090905 Re: CVE request: kernel: tc: uninitialised kernel memory leak
No Description Provided	Broken Link git.kernel.org text/html Inactive Link Not Archived	CONFIRM git.kernel.org/?p=linux/kernel/git/stable/linux-2.4.37.y.git;a=commit;h=096ed17f20affc2db0e307658c69b67433992a7a
USN-864-1: Linux kernel vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-864-1
Support	Third Party Advisory www.redhat.com text/html	REDHAT RHSA-2009:1522
Bug 520990 – CVE-2009-3228 kernel: tc: uninitialised kernel memory leak	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=520990
Linux Kernel tc_fill_tclass() Discloses Potentially Sensitive Kernel Memory to Local Users - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1023073
rhn.redhat.com | Red Hat Support	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2009:1548
Repository / Oval Repository	Third Party Advisory oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:9409
Support / Security / Advisories / / MDVSA-2010:198 | Mandriva	Third Party Advisory www.mandriva.com text/html	MANDRIVA MDVSA-2010:198
oss-security - Re: CVE request: kernel: tc: uninitialised kernel memory leak	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20090916 Re: CVE request: kernel: tc: uninitialised kernel memory leak
404: File not found	Broken Link www.kernel.org text/plain Inactive Link Not Archived	CONFIRM www.kernel.org/pub/linux/kernel/v2.6/testing/v2.6.31/ChangeLog-2.6.31-rc9

Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2009:1540
VMware vMA Update for Multiple Packages - Advisories - Community	Third Party Advisory web.archive.org text/html	SECUNIA 38794
oss-security - Re: CVE request: kernel: tc: uninitialised kernel memory leak	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20090907 Re: CVE request: kernel: tc: uninitialised kernel memory leak
oss-security - Re: CVE request: kernel: tc: uninitialised kernel memory leak	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20090906 Re: CVE request: kernel: tc: uninitialised kernel memory leak
[Security-announce] VMSA-2010-0004 ESX Service Console and vMA third party updates	Third Party Advisory lists.vmware.com text/html	MLIST [security-announce] 20100303 VMSA-2010-0004 ESX Service Console and vMA third party updates
tc: Fix unitialized kernel memory leak - Patchwork	Patch Third Party Advisory patchwork.ozlabs.org text/html	CONFIRM patchwork.ozlabs.org/patch/32830/
404: File not found	Broken Link www.kernel.org text/plain Inactive Link Not Archived	CONFIRM www.kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.37.6
VMware ESX Server 4 Multiple Vulnerabilities - Advisories - Community	Third Party Advisory web.archive.org text/html	SECUNIA 38834

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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	9.10	All	All	All

System						
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	9.10	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	2.6.31	-	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc8	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	2.6.31	-	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc5	All	All
Operating	Linux	Linux Kernel	2.6.31	rc6	All	All

System						
Operating System	Linux	Linux Kernel	2.6.31	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.31	rc8	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	5.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	5.4	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:6.06:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:6.06:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.10:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:-:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc7:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc8:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:-:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc7:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.31:rc8:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:5.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:5.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:5.0:*:*:*:*:*:*:*:

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report