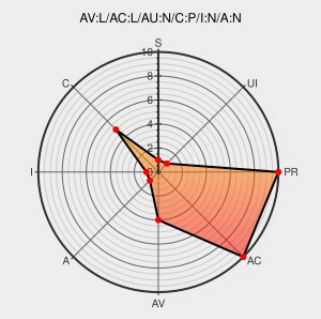
CVE-2010-3477

Published on: 09/21/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:02 PM UTC

CVE-2010-3477

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



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

The tcf_act_police_dump function in net/sched/act_police.c in the actions implementation in the network queueing functionality in the Linux kernel before 2.6.36-rc4 does not properly initialize certain structure members, which allows local users to obtain potentially sensitive information from kernel memory via vectors involving a dump operation. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-2942.

CVE-2010-3477 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
No Description Provided	Patch, Vendor Advisory, git.kernel.org, text/html, Inactive Link, Not Archived	CONFIRM git.kernel.org/?p=linux/kernel/git/davem/net-2.6.git;a=commit;h=0f04cfd098fb81fded74e78ea1a1b86cc6c6c31e
404: File not found	Broken Link, Third Party Advisory, www.kernel.org, text/plain, Inactive Link, Not Archived	CONFIRM www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.36-rc4
Support	Third Party Advisory	REDHAT RHSA-2010:0779

	www.redhat.com text/html	
SecurityTracker.com Archives - Linux Kernel tcf_act_police_dump() Function Lets Local Users Obtain Portions of Kernel Memory	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1024603
SecurityFocus	Third Party Advisory VDB Entry www.securityfocus.com text/html	BUGTRAQ 20111013 VMSA-2011-0012 VMware ESXi and ESX updates to third party libraries and ESX Service Console
USN-1000-1: Linux kernel vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-1000-1
Support	Third Party Advisory www.redhat.com text/html	REDHAT RHSA-2010:0839
VMSA-2011-0012.2	Third Party Advisory www.vmware.com text/html	CONFIRM www.vmware.com/security/advisories/VMSA-2011-0012.html
Red Hat update for kernel - Advisories - Community	Third Party Advisory web.archive.org text/html	SECUNIA 42890
About Secunia Research | Flexera	Third Party Advisory secunia.com Depreciated Link text/plain	SECUNIA 46397
Debian -- Security Information -- DSA-2126-1 linux-2.6	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-2126
access.redhat.com	Third Party Advisory www.redhat.com text/html	REDHAT RHSA-2011:0007

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	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All

System						
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	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	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	2.6.36	-	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc3	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	2.6.36	-	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc3	All	All

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.10:*:*:*:*:*:*:*:

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:9.04:*:*:*:*:*:*:*:

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

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.10:*:*:*:*:*:*:*:

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:9.04:*:*:*:*:*:*:*:

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

cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*:

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

cpe:2.3:o:linux:linux_kernel:2.6.36:-:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.36:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.36:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.36:rc3:*:*:*:*:*:*:

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

cpe:2.3:o:linux:linux_kernel:2.6.36:-:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.36:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.36:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.36:rc3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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