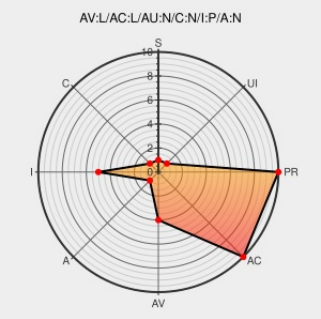
CVE-2010-3850

Published on: 12/30/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:26:00 AM UTC

CVE-2010-3850

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



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

The ec_dev_ioctl function in net/econet/af_econet.c in the Linux kernel before 2.6.36.2 does not require the CAP_NET_ADMIN capability, which allows local users to bypass intended access restrictions and configure econet addresses via an SIOCSIFADDR ioctl call.

CVE-2010-3850 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
[security-announce] SUSE Security Announcement: Realtime Linux Kernel (S	Mailing List, Third Party Advisory, lists.opensuse.org, text/html	SUSE SUSE-SA:2011:007
SUSE update for kernel - Advisories - Community	Third Party Advisory, web.archive.org, text/html	SECUNIA 43291
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory, www.vupen.com, text/html	VUPEN ADV-2011-0375
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	Mailing List, Third Party Advisory, lists.opensuse.org, text/html	SUSE SUSE-SA:2011:005

404: File not found	Broken Link www.kernel.org text/plain Inactive Link Not Archived	CONFIRM www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.36.2
SUSE update for kernel - Secunia.com	Third Party Advisory web.archive.org text/html	SECUNIA 43056
NEOHAPSIS - Peace of Mind Through Integrity and Insight	Broken Link archives.neohapsis.com text/x-c Inactive Link Not Archived	FULLDISC 20101207 Linux kernel exploit
USN-1023-1: Linux kernel vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-1023-1
Webmail - OVH	Third Party Advisory www.vupen.com text/html	VUPEN ADV-2011-0213
kernel/git/torvalds/linux.git - Linux kernel source tree	web.archive.org text/html Inactive Link Not Archived	MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=16c41745c7b92a243d0874f534c1655196c64b74
Support / Security / Advisories / / MDVSA-2010:257 | Mandriva	Third Party Advisory www.mandriva.com text/html	MANDRIVA MDVSA-2010:257
Bug 644156 – CVE-2010-3848 CVE-2010-3849 CVE-2010-3850 kernel: multiple vulnerabilities in Linux AF_ECONET	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=644156
Debian -- Security Information -- DSA-2126-1 linux-2.6	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-2126
oss-security - kernel: Multiple vulnerabilities in AF_ECONET	Mailing List Patch Third Party Advisory openwall.com text/html	MLIST [oss-security] 20101129 kernel: Multiple vulnerabilities in AF_ECONET
mandriva.com	Third Party Advisory www.mandriva.com text/html	MANDRIVA MDVSA-2011:051
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	VUPEN ADV-2011-0298
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SA:2011:008

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
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	9.10	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	All	All	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp3	All	All
Operating System	Suse	Linux Enterprise Real Time Extension	11	sp1	All	All
Operating System	Suse	Linux Enterprise Real Time Extension	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	10	sp3	All	All
Operating System	Suse	Linux Enterprise Server	9	All	All	All

Operating System	Suse	Linux Enterprise Server	10	sp3	All	All
Operating System	Suse	Linux Enterprise Server	9	All	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	10	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	10	sp3	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:9.10:*:*:*:*:*:*:*:

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:9.10:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:10:sp3:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:10:sp3:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_real_time_extension:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_real_time_extension:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:10:sp3:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:9:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:10:sp3:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:9:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_software_development_kit:10:sp3:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_software_development_kit:10:sp3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→