



CVE-2012-2313

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2012-2313
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-13 10:24:00 UTC
Updated	2023-02-13 00:24:00 UTC
Description	The rio_ioctl function in drivers/net/ethernet/dlink/dl2k.c in the Linux kernel before 3.3.7 does not restrict access to the SIOC

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	3.3	All	All	All
Operating System	Linux	Linux Kernel	3.3	rc1	All	All
Operating System	Linux	Linux Kernel	3.3	rc2	All	All
Operating System	Linux	Linux Kernel	3.3	rc3	All	All
Operating System	Linux	Linux Kernel	3.3	rc4	All	All
Operating System	Linux	Linux Kernel	3.3	rc5	All	All
Operating System	Linux	Linux Kernel	3.3	rc6	All	All
Operating System	Linux	Linux Kernel	3.3	rc7	All	All
Operating System	Linux	Linux Kernel	3.3.1	All	All	All
Operating System	Linux	Linux Kernel	3.3.2	All	All	All
Operating System	Linux	Linux Kernel	3.3.3	All	All	All
Operating System	Linux	Linux Kernel	3.3.4	All	All	All
Operating System	Linux	Linux Kernel	3.3.5	All	All	All
Operating System	Linux	Linux Kernel	3.3	All	All	All
Operating System	Linux	Linux Kernel	3.3	rc1	All	All
Operating System	Linux	Linux Kernel	3.3	rc2	All	All
Operating System	Linux	Linux Kernel	3.3	rc3	All	All

Operating System	Linux	Linux Kernel	3.3	rc4	All	All
Operating System	Linux	Linux Kernel	3.3	rc5	All	All
Operating System	Linux	Linux Kernel	3.3	rc6	All	All
Operating System	Linux	Linux Kernel	3.3	rc7	All	All
Operating System	Linux	Linux Kernel	3.3.1	All	All	All
Operating System	Linux	Linux Kernel	3.3.2	All	All	All
Operating System	Linux	Linux Kernel	3.3.3	All	All	All
Operating System	Linux	Linux Kernel	3.3.4	All	All	All
Operating System	Linux	Linux Kernel	3.3.5	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	10.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Server	10.0	sp4	All	All
Operating System	Redhat	Enterprise Linux	5	All	server	All
Operating System	Redhat	Enterprise Linux	5	All	server	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	client	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	client	All
Operating System	Redhat	Enterprise Linux Eus	5.6.z	All	server	All
Operating System	Redhat	Enterprise Linux Eus	5.6.z	All	server	All
Operating System	Redhat	Enterprise Linux Long Life	5.6	All	server	All
Operating System	Redhat	Enterprise Linux Long Life	5.6	All	server	All
Operating System	Redhat	Enterprise Linux Server Aus	6.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.1.z	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.2.z	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.1.z	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.2.z	All	All	All

References

Reference	Source	Link
[security-announce] SUSE-SU-2015:0812-1: important: Security update for	SUSE	lists.opens
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.c
818820 – (CVE-2012-2313) CVE-2012-2313 kernel: unfiltered netdev rio_ioctl access by users	CONFIRM	bugzilla.re
Red Hat Customer Portal	REDHAT	rhn.redhat.
'[security bulletin] HPSBGN02970 rev.1 - HP Rapid Deployment Pack (RDP) or HP Insight Control Server ' - MARC	HP	marc.info
Linux Kernel dl2k Network Driver IOCTL Handling Local Denial of Service Vulnerability	BID	www.secu
	CONFIRM	

kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.c
Red Hat Customer Portal	REDHAT	rhn.redhat.
Red Hat Customer Portal	REDHAT	rhn.redhat.
oss-security - Re: CVE Request: more tight ioctl permissions in dl2k driver	MLIST	www.open
www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.3.7	CONFIRM	www.kerne
Red Hat Customer Portal	REDHAT	rhn.redhat.
dl2k: Clean up rio_ioctl · torvalds/linux@1bb57e9 · GitHub	CONFIRM	github.com
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](#).

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