



CVE-2014-9715

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2014-9715
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-27 10:59:00 UTC
Updated	2023-11-07 02:23:00 UTC
Description	include/net/netfilter/nf_contrack_extend.h in the netfilter subsystem in the Linux kernel before 3.14.5 uses an insufficiently

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
'OOPS NULL pointer dereference in nf_nat_setup_info+0x471 (reproducible, 3.14.4)' - MARC	MLIST	marc.info
www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.14.5	CONFIRM	www.kernel.org
Bug 1208684 – CVE-2014-9715 kernel: netfilter connection tracking extensions denial of service	CONFIRM	bugzilla.redhat.com
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
Debian -- Security Information -- DSA-3237-1 linux	DEBIAN	www.debian.org
Linux Kernel 'nf_contrack_extend.h' NULL Pointer Dereference Denial of Service Vulnerability	BID	www.securityfocus.com
Red Hat Customer Portal	REDHAT	rhn.redhat.com
oss-security - CVE request netfilter connection tracking accounting.	MLIST	www.openwall.com
Oracle Linux Bulletin - January 2016	CONFIRM	www.oracle.com
Red Hat Customer Portal	REDHAT	rhn.redhat.com
netfilter: nf_contrack: reserve two bytes for nf_ct_ext->len · torvalds/linux@223b02d · GitHub	CONFIRM	github.com
kernel/git/torvalds/linux.git - Linux kernel source tree		git.kernel.org
Linux Kernel Netfilter Connection Tracking Accounting Bug Lets Local Users Deny Service - SecurityTracker	SECTRACK	www.securitytra

CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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.

Free CVE JSON API cve.report/api

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