



CVE-2014-0131

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

Summary

CVE	CVE-2014-0131
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-03-24 16:40:00 UTC
Updated	2023-02-13 00:32:00 UTC
Description	Use-after-free vulnerability in the skb_segment function in net/core/skbuff.c in the Linux kernel through 3.13.6 allows attackers to trigger a kernel panic via a crafted packet.

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Opensuse	Evergreen	11.4	All	All	All
Operating System	Opensuse	Evergreen	11.4	All	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All

References

Reference	Source	Link	Tags
oss-security - CVE-2014-0131 -- kernel: net: use-after-free during segmentation with zerocopy	MLIST	www.openwall.com	Mailing L
[PATCH 5/5] skbuff: skb_segment: orphan frags before copying — Linux Network Development	MLIST	www.spinics.net	Mailing L
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	Patch, V
Bug 1074589 – CVE-2014-0131 kernel: net: use-after-free during segmentation with zerocopy	CONFIRM	bugzilla.redhat.com	Issue Tr
[security-announce] openSUSE-SU-2015:0566-1: important: kernel update fo	SUSE	lists.opensuse.org	Third Pa
skbuff: skb_segment: orphan frags before copying · torvalds/linux@1fd819e · GitHub	CONFIRM	github.com	Patch, V
[security-announce] SUSE-SU-2015:0481-1: important: Security update for	SUSE	lists.opensuse.org	Third Pa
[PATCH 0/5] skbuff: fix skb_segment with zero copy skbs — Linux Network Development	MLIST	www.spinics.net	Mailing L
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	

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

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