



CVE-2017-5970

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

Summary

CVE	CVE-2017-5970
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-14 06:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	The ipv4_pktinfo_prepare function in net/ipv4/ip_sockglue.c in the Linux kernel through 4.9.9 allows attackers to cause a de

Risk And Classification

Problem Types: CWE-476

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	Tags
oss-security - Fwd: [scr293903] Linux kernel - upstream	MLIST	www.openwall.com	Mailing Lis
Red Hat Customer Portal	REDHAT	access.redhat.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	
Android Security Bulletin—July 2017 Android Open Source Project	CONFIRM	source.android.com	
[PATH,net] ipv4: keep skb->dst around in presence of IP options - Patchwork	CONFIRM	patchwork.ozlabs.org	Patch, Thi
ipv4: keep skb->dst around in presence of IP options · torvalds/linux@34b2cef · GitHub	CONFIRM	github.com	Issue Trac
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	Issue Trac
Bug 1421638 – CVE-2017-5970 kernel: ipv4: Invalid IP options could cause skb->dst drop	CONFIRM	bugzilla.redhat.com	Issue Trac
Linux kernel 'ip_sockglue.c' Denial of Service Vulnerability	BID	www.securityfocus.com	
Debian -- Security Information -- DSA-3791-1 linux	DEBIAN	www.debian.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
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](#)