



CVE-2017-6347

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

Summary

CVE	CVE-2017-6347
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-01 20:59:00 UTC
Updated	2023-02-10 00:53:00 UTC
Description	The ip_msg_recv_checksum function in net/ipv4/ip_sockglue.c in the Linux kernel before 4.10.1 has incorrect expectations

Risk And Classification

Problem Types: CWE-125

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	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	Tags
1427984 – (CVE-2017-6347) CVE-2017-6347 kernel: ipv4: Incorrect IP_CHECKSUM handling	CONFIRM	bugzilla.redhat.com	Issue
oss-security - Linux: ip: fix IP_CHECKSUM handling (CVE-2017-6347)	MLIST	www.openwall.com	Maili
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.10.1	CONFIRM	www.kernel.org	Patch
ip: fix IP_CHECKSUM handling · torvalds/linux@ca4ef45 · GitHub	CONFIRM	github.com	Patch
Linux Kernel CVE-2017-6347 Denial of Service Vulnerability	BID	www.securityfocus.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

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](#)