



CVE-2017-7308

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

Summary

CVE	CVE-2017-7308
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-29 20:59:00 UTC
Updated	2023-02-14 18:32:00 UTC
Description	The packet_set_ring function in net/packet/af_packet.c in the Linux kernel through 4.10.6 does not properly validate certain

Risk And Classification

Problem Types: CWE-787 | CWE-681

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
[net,v2,1/3] net/packet: fix overflow in check for priv area size - Patchwork	CONFIRM	patchwork.ozlabs.org
Red Hat Customer Portal	REDHAT	access.redhat.com
Project Zero: Exploiting the Linux kernel via packet sockets	MISC	googleprojectzero.blogspot.com
Linux 4.8.0 < 4.8.0-46 - AF_PACKET packet_set_ring Privilege Escalation (Metasploit) - Linux local Exploit	EXPLOIT-DB	www.exploit-db.com
Red Hat Customer Portal	REDHAT	access.redhat.com
[net,v2,3/3] net/packet: fix overflow in check for tp_reserve - Patchwork	CONFIRM	patchwork.ozlabs.org
Android Security Bulletin—July 2017 Android Open Source Project	CONFIRM	source.android.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Red Hat Customer Portal	REDHAT	access.redhat.com
[net,v2,2/3] net/packet: fix overflow in check for tp_frame_nr - Patchwork	CONFIRM	patchwork.ozlabs.org
Linux kernel CVE-2017-7308 Local Denial of Service Vulnerability	BID	www.securityfocus.com
Linux Kernel 4.8.0 (Ubuntu) - Packet Socket Local Privilege Escalation	EXPLOIT-DB	www.exploit-db.com

CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
No vendor comments have been submitted for this CVE.		
Legacy QID Mappings		
378249 Virtuozzo Linux Security Update for kernel-tools-libs (VZLSA-2017:1308)		

© [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 registred 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