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

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)