CVE-2017-14497

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-14497
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-15 18:29:00 UTC
Updated	2023-01-19 15:48:00 UTC
Description	The tpacket_rcv function in net/packet/af_packet.c in the Linux kernel before 4.13 mishandles vnet headers, which might all

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source
'[PATCH] packet: Don't write vnet header beyond end of buffer' - MARC	CONFIR
Linux Kernel Buffer Overflow in tpacket_rcv() Lets Local Users Cause Denial of Service Conditions - SecurityTracker	SECTR
Google Android Bugs Let Remote Users Obtain Sensitive Information, Deny Service, and Execute Arbitrary Code - SecurityTracker	SECTR
packet: Don't write vnet header beyond end of buffer · torvalds/linux@edbd58b · GitHub	CONFIR
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIR
1492593 – (CVE-2017-14497) CVE-2017-14497 kernel: buffer overflow in tpacket_rcv() in net/packet/af_packet.c	CONFIR
Linux Kernel CVE-2017-14497 Local Buffer Overflow Vulnerability	BID
oss-sec: CVE-2017-14497: Linux kernel: packet: buffer overflow in tpacket_rcv()	MLIST
Debian -- Security Information -- DSA-3981-1 linux	DEBIAN
Android Security Bulletin—January 2018 | Android Open Source Project	CONFIR

'[PATCH] packet: Don't write vnet header beyond end of buffer' thread - MARC	CONFIR
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.