CVE-2017-7487

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

Summary

CVE	CVE-2017-7487
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-14 22:29:00 UTC
Updated	2023-02-14 21:37:00 UTC
Description	The ipxitf_ioctl function in net/ipx/af_ipx.c in the Linux kernel through 4.11.1 mishandles reference counts, which allows loca

Risk And Classification

Problem Types: CWE-416

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
Android Security Bulletin—September 2017 | Android Open Source Project
Linux kernel 'net/ipx/af_ipx.c' Use After Free Local Denial of Service Vulnerability
Bug 1447734 – CVE-2017-7487 kernel: Reference counter leak in ipxitf_ioctl resulting into use after free
Debian -- Security Information -- DSA-3886-1 linux
ipx: call ipxitf_put() in ioctl error path - Patchwork
ipx: call ipxitf_put() in ioctl error path · torvalds/linux@ee0d8d8 · GitHub
Linux Kernel Use-After-Free Memory Error in ipxitf_ioctl() Lets Local Users Cause Denial of Service Conditions on the Target System - Securit
kernel/git/torvalds/linux.git - Linux kernel source tree
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**