CVE-2016-10200

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

Summary

CVE	CVE-2016-10200
State	PUBLIC
Assigner	security@android.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-07 21:59:00 UTC
Updated	2023-06-07 12:44:00 UTC
Description	Race condition in the L2TPv3 IP Encapsulation feature in the Linux kernel before 4.8.14 allows local users to gain privileges

Risk And Classification

Problem Types: CWE-264 | CWE-362 | CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference
Red Hat Customer Portal
l2tp: fix racy SOCK_ZAPPED flag check in l2tp_ip{,6}_bind() · torvalds/linux@32c2311 · GitHub
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.8.14
Red Hat Customer Portal
Android Multiple Flaws Let Users Deny Service, Obtain Potentially Sensitive Information, and Gain Elevated Privileges and Let Remote Users
Linux Kernel l2tp_ip6_bind() Race Condition Lets Local Users Deny Service or Gain Elevated Privileges - SecurityTracker
Red Hat Customer Portal
Android Security Bulletin—March 2017 | Android Open Source Project
Linux Kernel CVE-2016-10200 Multiple Privilege Escalation Vulnerabilities
Red Hat Customer Portal
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**