



CVE-2019-17666

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

Summary

CVE	CVE-2019-17666
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-17 02:15:00 UTC
Updated	2023-11-07 03:06:00 UTC
Description	rtl_p2p_noa_ie in drivers/net/wireless/realtek/rtlwifi/ps.c in the Linux kernel through 5.3.6 lacks a certain upper-bound check

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference

- Nico Waisman na Twitterze: "Found this bug on Monday. An overflow on the linux rtlwifi driver on P2P (Wifi-Direct), while parsing Notice of Ab
- LKML: Laura Abbott: [PATCH] rtlwifi: Fix potential overflow on P2P code
- Red Hat Customer Portal
- [SECURITY] Fedora 31 Update: kernel-5.3.7-301.fc31 - package-announce - Fedora Mailing-Lists
- [security-announce] openSUSE-SU-2019:2392-1: important: Security update
- Red Hat Customer Portal

