CVE-2022-1204

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-1204
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-29 15:15:00 UTC
Updated	2022-09-02 19:41:00 UTC
Description	A use-after-free flaw was found in the Linux kernel's Amateur Radio AX.25 protocol functionality in the way a user connects

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	10.0	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.17	rc1	All	All
Operating System	Linux	Linux Kernel	5.17	rc2	All	All

References

Reference	Source	Link
2071051 – (CVE-2022-1204) CVE-2022-1204 kernel: Use after free in net/ax25/af_ax25.c	MISC	bugzilla.redhat.c
oss-security - CVE-2022-1204: Linux kernel: UAF caused by binding operation when ax25 device is detaching	MISC	www.openwall.c
CVE-2022-1204	MISC	security-tracker.
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.c
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

- 179258 Debian Security Update for linux (DSA 5127-1)
- 180605 Debian Security Update for linux (DSA 5173-1)
- 182062 Debian Security Update for linux (CVE-2022-1204)
- 198822 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5469-1)
- 198857 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5514-1)
- 198858 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5515-1)
- 198875 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5539-1)
- 282604 Fedora Security Update for kernel (FEDORA-2022-8efcea6e67)
- 282605 Fedora Security Update for kernel (FEDORA-2022-0816754490)
- 355563 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-036
- 376925 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0125)
- 6140155 AWS Bottlerocket Security Update for kernel (GHSA-3gmh-p94w-pj3p)
- 671817 EulerOS Security Update for kernel (EulerOS-SA-2022-1868)
- 672003 EulerOS Security Update for kernel (EulerOS-SA-2022-2134)
- 903725 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10777)
- 903853 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10760)
- 904211 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10777-1)
- 904722 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10760-1)
- 905986 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10777-2)
- 906271 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10760-2)