



CVE-2022-41848

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

Summary

CVE	CVE-2022-41848
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-30 06:15:00 UTC
Updated	2023-11-07 03:53:00 UTC
Description	drivers/char/pcmcia/synclink_cs.c in the Linux kernel through 5.19.12 has a race condition and resultant use-after-free if a p

Risk And Classification

Problem Types: CWE-362 | CWE-416

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
[PATCH v5] char: pcmcia: synclink_cs: Fix use-after-free in mgslpc_ops	MISC	lore.kernel.org	
[PATCH v5] char: pcmcia: synclink_cs: Fix use-after-free in mgslpc_ops		lore.kernel.org	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[752669](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3587-1)

[752671](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3584-1)

[752700](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3688-1)

[752702](#) SUSE Enterprise Linux Securityv Update for the Linux Kernel (SUSE-SU-2022:3693-1)

752702 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3704-1)
752708 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3704-1)
752724 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3775-1)
752750 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3844-1)
753060 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4615-1)
753063 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4617-1)
753095 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3585-1)
753370 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3609-1)
753374 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3809-1)
753703 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0416-1)
753707 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0416-1)
753727 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0416-1)
904087 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11085)
904111 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11079)
907118 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11085-1)
907172 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11079-1)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)