



CVE-2023-2177

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

Summary

CVE	CVE-2023-2177
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-20 21:15:00 UTC
Updated	2023-04-28 03:48:00 UTC
Description	A null pointer dereference issue was found in the sctp network protocol in net/sctp/stream_sched.c in Linux Kernel. If stream

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.19	rc1	All	All
Operating System	Linux	Linux Kernel	5.19	rc2	All	All
Operating System	Linux	Linux Kernel	5.19	rc3	All	All
Operating System	Linux	Linux Kernel	5.19	rc4	All	All
Operating System	Linux	Linux Kernel	5.19	rc5	All	All
Operating System	Linux	Linux Kernel	5.19	rc6	All	All
Operating System	Linux	Linux Kernel	5.19	rc7	All	All
Operating System	Linux	Linux Kernel	5.19	rc8	All	All

References

Reference	Source	Link	Tags
kernel/git/netdev/net.git - Netdev Group's networking 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

181863	Debian Security Update for linux (CVE-2023-2177)
242617	Red Hat Update for kernel (RHSA-2023:7398)
355199	Amazon Linux Security Advisory for kernel : ALAS2023-2023-070
378710	Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0079)
379043	Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0136)
673214	EulerOS Security Update for kernel (EulerOS-SA-2023-2383)
673232	EulerOS Security Update for kernel (EulerOS-SA-2023-2357)
673261	EulerOS Security Update for kernel (EulerOS-SA-2023-2614)
673272	EulerOS Security Update for kernel (EulerOS-SA-2023-2584)
673393	EulerOS Security Update for kernel (EulerOS-SA-2023-2647)
673498	EulerOS Security Update for kernel (EulerOS-SA-2023-3132)
674113	EulerOS Security Update for kernel (EulerOS-SA-2023-2689)
755043	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3988-1)
755061	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4030-1)
755082	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4058-1)
755083	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4057-1)
755085	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4072-1)
755086	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4071-1)
755096	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4093-1)
755107	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4095-1)
755229	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4072-2)
906922	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (26316-1)
906979	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (26313-1)

© [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](#)