CVE-2021-38185

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-38185
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-08 00:15:00 UTC
Updated	2023-06-04 22:15:00 UTC
Description	GNU cpio through 2.13 allows attackers to execute arbitrary code via a crafted pattern file, because of a dstring.c ds_fgetstr

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Cpio	All	All	All	All

References

Reference	Source	Link
GitHub - fangqyi/cpiopwn: ACE poc exploit for glibc cpio 2.13 through mmap chunk metadata curruption	MISC	github.com
cpio.git - GNU cpio	MISC	git.savannah.gnu.org
cpio RCE Exploit Caused by Integer Overflow	MISC	lists.gnu.org
[SECURITY] [DLA 3445-1] cpio security update	MLIST	lists.debian.org
Re: cpio RCE Exploit Caused by Integer Overflow	MISC	lists.gnu.org
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

159796 Oracle Enterprise Linux Security Update for cpio (ELSA-2022-1991)

181827 Debian Security Update for cpio (DLA 3445-1)

183753 Debian Security Update for cpio (CVE-2021-38185)

198484 Ubuntu Security Notification for GNU cpio Vulnerability (USN-5064-1)

199639 Ubuntu Security Notification for GNU cpio Vulnerability (USN-5064-3)

240271 Red Hat Update for cpio (RHSA-2022:1991)

354707 Amazon Linux Security Advisory for cpio : ALAS2022-2023-263

354786 Amazon Linux Security Advisory for cpio : ALAS2-2023-1972

355140 Amazon Linux Security Advisory for cpio : ALAS2023-2023-021

501831 Alpine Linux Security Update for cpio

504656 Alpine Linux Security Update for cpio

670812 EulerOS Security Update for cpio (EulerOS-SA-2021-2706)

670946 EulerOS Security Update for cpio (EulerOS-SA-2021-2681)

671036 EulerOS Security Update for cpio (EulerOS-SA-2021-2654)

671045 EulerOS Security Update for cpio (EulerOS-SA-2021-2626)

750962 SUSE Enterprise Linux Security Update for cpio (SUSE-SU-2021:2686-1)

750966 SUSE Enterprise Linux Security Update for cpio (SUSE-SU-2021:2689-1)

750968 OpenSUSE Security Update for cpio (openSUSE-SU-2021:2689-1)

750996 SUSE Enterprise Linux Security Update for cpio (SUSE-SU-2021:2808-1)

900299 CBL-Mariner Linux Security Update for cpio 2.13

901141 Common Base Linux Mariner (CBL-Mariner) Security Update for cpio (6357)

902078 Common Base Linux Mariner (CBL-Mariner) Security Update for cpio (6357-1)

903152 Common Base Linux Mariner (CBL-Mariner) Security Update for cpio (5208)

940501 AlmaLinux Security Update for cpio (ALSA-2022:1991)

960367 Rocky Linux Security Update for cpio (RLSA-2022:1991)

CVE.report and Source URL Uptime Status status.cve.report