



CVE-2022-42703

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

Summary

CVE	CVE-2022-42703
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-09 23:15:00 UTC
Updated	2023-02-03 20:29:00 UTC
Description	mm/rmap.c in the Linux kernel before 5.19.7 has a use-after-free related to leaf anon_vma double reuse.

Risk And Classification

Problem Types: 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
2351 - project-zero - Project Zero - Monorail	MISC	bugs.chromium.org
Project Zero: Exploiting CVE-2022-42703 - Bringing back the stack attack	MISC	googleprojectzero.blogspot.com
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.19.7	MISC	cdn.kernel.org
mm/rmap: Fix anon_vma->degree ambiguity leading to double-reuse · torvalds/linux@2555283 · GitHub	MISC	github.com
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

160503 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-1091)

160583 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-2458)

160692 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-2951)
181120 Debian Security Update for linux (CVE-2022-42703)
199029 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5728-1)
199037 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5728-2)
199051 Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5728-3)
199056 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5757-1)
199057 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5755-1)
199059 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5756-1)
199060 Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-5756-2)
199061 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5755-2)
199070 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5756-3)
199072 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5774-1)
199073 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5773-1)
199078 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5779-1)
199084 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5789-1)
199573 Ubuntu Security Notification for Linux kernel Vulnerability (USN-5916-1)
241243 Red Hat Update for kernel-rt (RHSA-2023:1092)
241249 Red Hat Update for kernel (RHSA-2023:1091)
241417 Red Hat Update for kernel security (RHSA-2023:2458)
241468 Red Hat Update for kernel-rt (RHSA-2023:2148)
241504 Red Hat Update for kernel security (RHSA-2023:2951)
241527 Red Hat Update for kernel-rt (RHSA-2023:2736)
241567 Red Hat Update for kernel security (RHSA-2023:3388)
241823 Red Hat Update for kernel (RHSA-2023:4137)
241830 Red Hat Update for kernel-rt (RHSA-2023:4138)
257226 CentOS Security Update for kernel (CESA-2023:1091)
378468 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-20230042)
378473 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0021)
378510 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0043)

378512 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0042)
610501 Google Android August 2023 Security Patch Missing for Samsung
610502 Google Android August 2023 Security Patch Missing for Huawei EMUI
610504 Google Android Devices July 2023 Security Patch Missing
672410 EulerOS Security Update for kernel (EulerOS-SA-2022-2796)
672454 EulerOS Security Update for kernel (EulerOS-SA-2022-2848)
672474 EulerOS Security Update for kernel (EulerOS-SA-2022-2823)
672495 EulerOS Security Update for kernel (EulerOS-SA-2023-1012)
672516 EulerOS Security Update for kernel (EulerOS-SA-2023-1037)
672532 EulerOS Security Update for kernel (EulerOS-SA-2023-1126)
672564 EulerOS Security Update for kernel (EulerOS-SA-2023-1102)
672711 EulerOS Security Update for kernel (EulerOS-SA-2023-1507)
752814 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 31 for SLE 15 SP1) (SUSE-SU-2022:4112-1)
752831 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 31 for SLE 15) (SUSE-SU-2022:4027-1)
752839 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3929-1)
752850 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 1 for SLE 15 SP4) (SUSE-SU-2022:4035-1)
752852 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 16 for SLE 15 SP3) (SUSE-SU-2022:4100-1)
752874 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 32 for SLE 15 SP1) (SUSE-SU-2022:4024-1)
752875 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 2 for SLE 15 SP4) (SUSE-SU-2022:4039-1)
752880 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4053-1)
752889 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3897-1)
752894 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 22 for SLE 15 SP3) (SUSE-SU-2022:4033-1)
752902 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 30 for SLE 15) (SUSE-SU-2022:4129-1)
752904 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 23 for SLE 15 SP3) (SUSE-SU-2022:4034-1)
752911 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3998-1)
752913 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4072-1)
752915 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 33 for SLE 15 SP1) (SUSE-SU-2022:4030-1)
752930 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 0 for SLE 15 SP4) (SUSE-SU-2022:4113-1)
752944 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4273-1)

752959 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4272-1)
753038 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4573-1)
753039 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4574-1)
753051 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4589-1)
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)
904169 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11095)
904175 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11094)
904375 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11095-1)
904400 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11094-1)
905923 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11095-2)
906488 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11094-2)
941023 AlmaLinux Security Update for kernel (ALSA-2023:2458)
941061 AlmaLinux Security Update for kernel-rt (ALSA-2023:2148)
941096 AlmaLinux Security Update for kernel (ALSA-2023:2951)
941114 AlmaLinux Security Update for kernel-rt (ALSA-2023:2736)

© [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](#)