



CVE-2019-19769

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

Summary

CVE	CVE-2019-19769
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-12 20:15:00 UTC
Updated	2023-11-07 03:07:00 UTC
Description	In the Linux kernel 5.3.10, there is a use-after-free (read) in the perf_trace_lock_acquire function (related to include/trace/ev

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 30 Update: kernel-tools-5.5.16-100.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
USN-4368-1: Linux kernel vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
December 2019 Linux Kernel Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
[SECURITY] Fedora 31 Update: kernel-5.5.11-200.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 30 Update: kernel-tools-5.5.16-100.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
205705 – Linux Kernel 5.3.10 - perf_trace_lock_acquire use-after-free	MISC	bugzilla.kernel.org
USN-4369-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
[SECURITY] Fedora 31 Update: kernel-5.5.11-200.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[174896](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1177-1)

[174917](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1211-1)

[174919](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1238-1)

[750199](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0758-1)

[750276](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0532-1)

[750650](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1975-1)

[750652](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1977-1)

[750762](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1977-1)

[750766](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1975-1)

© [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](#)