



CVE-2019-19602

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

Summary

CVE	CVE-2019-19602
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-05 14:15:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	fpregs_state_valid in arch/x86/include/asm/fpu/internal.h in the Linux kernel before 5.4.2, when GCC 9 is used, allows cont

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
runtime: memory corruption on Linux 5.3.x from async preemption · Issue #35777 · golang/go · GitHub	MISC	github.com
USN-4284-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.4.2	MISC	cdn.kernel.org
December 2019 Linux Kernel Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
x86/fpu: Don't cache access to fpu_fpregs_owner_ctx · torvalds/linux@59c4bd8 · GitHub	MISC	github.com
205663 – AVX register corruption from signal delivery	MISC	bugzilla.kernel.org
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159684](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2020-4431)

[940256](#) AlmaLinux Security Update for kernel (ALSA-2020:4431)

© [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](#)