



CVE-2020-14381

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

Summary

CVE	CVE-2020-14381
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-03 17:15:00 UTC
Updated	2020-12-08 16:00:00 UTC
Description	A flaw was found in the Linux kernel's futex implementation. This flaw allows a local attacker to corrupt system memory or e

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
Operating System	Linux	Linux Kernel	5.6	-	All	All
Operating System	Linux	Linux Kernel	5.6	rc1	All	All
Operating System	Linux	Linux Kernel	5.6	rc2	All	All
Operating System	Linux	Linux Kernel	5.6	rc3	All	All
Operating System	Linux	Linux Kernel	5.6	rc4	All	All
Operating System	Linux	Linux Kernel	5.6	rc5	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.6	-	All	All
Operating System	Linux	Linux Kernel	5.6	rc1	All	All
Operating System	Linux	Linux Kernel	5.6	rc2	All	All
Operating System	Linux	Linux Kernel	5.6	rc3	All	All
Operating System	Linux	Linux Kernel	5.6	rc4	All	All
Operating System	Linux	Linux Kernel	5.6	rc5	All	All

References

Reference	Source
-----------	--------

1874311 – (CVE-2020-14381) CVE-2020-14381 kernel: referencing inode of removed superblock in get_futex_key() causes UAF	MISC
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [159684](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2020-4431)
- [610357](#) Google Android Devices August 2021 Security Patch Missing
- [610366](#) Google Android September 2021 Security Patch Missing for Samsung
- [670744](#) EulerOS Security Update for kernel (EulerOS-SA-2021-2502)
- [900040](#) CBL-Mariner Linux Security Update for kernel 5.4.91
- [903162](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3650)
- [905965](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3650-1)
- [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](#)