



CVE-2020-13844

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

Summary

CVE	CVE-2020-13844
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-08 23:15:00 UTC
Updated	2022-04-28 19:30:00 UTC
Description	Arm Armv8-A core implementations utilizing speculative execution past unconditional changes in control flow may allow un

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Arm	Cortex-a32	-	All	All	All
Hardware	Arm	Cortex-a32	-	All	All	All
Operating System	Arm	Cortex-a32 Firmware	-	All	All	All
Operating System	Arm	Cortex-a32 Firmware	-	All	All	All
Hardware	Arm	Cortex-a34	-	All	All	All
Hardware	Arm	Cortex-a34	-	All	All	All
Operating System	Arm	Cortex-a34 Firmware	-	All	All	All
Operating System	Arm	Cortex-a34 Firmware	-	All	All	All
Hardware	Arm	Cortex-a35	-	All	All	All
Hardware	Arm	Cortex-a35	-	All	All	All
Operating System	Arm	Cortex-a35 Firmware	-	All	All	All
Operating System	Arm	Cortex-a35 Firmware	-	All	All	All
Hardware	Arm	Cortex-a53	-	All	All	All
Hardware	Arm	Cortex-a53	-	All	All	All
Operating System	Arm	Cortex-a53 Firmware	-	All	All	All
Operating System	Arm	Cortex-a53 Firmware	-	All	All	All
Hardware	Arm	Cortex-a57	-	All	All	All

Hardware	Arm	Cortex-a57	-	All	All	All
Operating System	Arm	Cortex-a57 Firmware	-	All	All	All
Operating System	Arm	Cortex-a57 Firmware	-	All	All	All
Hardware	Arm	Cortex-a72	-	All	All	All
Hardware	Arm	Cortex-a72	-	All	All	All
Operating System	Arm	Cortex-a72 Firmware	-	All	All	All
Operating System	Arm	Cortex-a72 Firmware	-	All	All	All
Hardware	Arm	Cortex-a73	-	All	All	All
Hardware	Arm	Cortex-a73	-	All	All	All
Operating System	Arm	Cortex-a73 Firmware	-	All	All	All
Operating System	Arm	Cortex-a73 Firmware	-	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All

References

Reference	Source	Link	Tags
[llvm-dev] Mitigating straight-line speculation vulnerability CVE-2020-13844	CONFIRM	lists.llvm.org	Mailing List, Third Party
Straight Line Speculation (SLS) mitigation.	CONFIRM	gcc.gnu.org	Patch, Third Party
[security-announce] openSUSE-SU-2020:1692-1: moderate: Security update f	SUSE	lists.opensuse.org	
developer.arm.com/support/arm-security-updates/speculative-processor-vulnerabil...	MISC	developer.arm.com	Vendor Advisory
Speculative Processor Vulnerability Frequently asked questions – Arm Developer	CONFIRM	developer.arm.com	Vendor Advisory
Speculative Processor Vulnerability – Arm Developer	CONFIRM	developer.arm.com	Vendor Advisory
[security-announce] openSUSE-SU-2020:1693-1: moderate: Security update f	SUSE	lists.opensuse.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 610406 Google Pixel Android April 2022 Security Patch Missing
- 750477 OpenSUSE Security Update for gcc7 (openSUSE-SU-2020:2300-1)
- 750478 OpenSUSE Security Update for gcc7 (openSUSE-SU-2020:2301-1)
- 755898 SUSE Enterprise Linux Security Update for gcc7 (SUSE-SU-2023:3662-1)

© [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](#)