



CVE-2022-23960

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

Summary

CVE	CVE-2022-23960
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-13 00:15:00 UTC
Updated	2023-01-20 02:34:00 UTC
Description	Certain Arm Cortex and Neoverse processors through 2022-03-08 do not properly restrict cache speculation, aka Spectre-F

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Arm	Cortex-a57	-	All	All	All
Operating System	Arm	Cortex-a57 Firmware	-	All	All	All
Hardware	Arm	Cortex-a65	-	All	All	All
Hardware	Arm	Cortex-a65ae	-	All	All	All
Operating System	Arm	Cortex-a65ae Firmware	-	All	All	All
Operating System	Arm	Cortex-a65 Firmware	-	All	All	All
Hardware	Arm	Cortex-a710	-	All	All	All
Operating System	Arm	Cortex-a710 Firmware	-	All	All	All
Hardware	Arm	Cortex-a72	-	All	All	All
Operating System	Arm	Cortex-a72 Firmware	-	All	All	All
Hardware	Arm	Cortex-a73	-	All	All	All
Operating System	Arm	Cortex-a73 Firmware	-	All	All	All
Hardware	Arm	Cortex-a75	-	All	All	All
Operating System	Arm	Cortex-a75 Firmware	-	All	All	All
Hardware	Arm	Cortex-a76	-	All	All	All
Hardware	Arm	Cortex-a76ae	-	All	All	All
Operating System	Arm	Cortex-a76ae Firmware	-	All	All	All

Operating System	Arm	Cortex-a76 Firmware	-	All	All	All
Hardware	Arm	Cortex-a77	-	All	All	All
Operating System	Arm	Cortex-a77 Firmware	-	All	All	All
Hardware	Arm	Cortex-a78	-	All	All	All
Hardware	Arm	Cortex-a78ae	-	All	All	All
Operating System	Arm	Cortex-a78ae Firmware	-	All	All	All
Operating System	Arm	Cortex-a78 Firmware	-	All	All	All
Hardware	Arm	Cortex-r7	-	All	All	All
Operating System	Arm	Cortex-r7 Firmware	-	All	All	All
Hardware	Arm	Cortex-r8	-	All	All	All
Operating System	Arm	Cortex-r8 Firmware	-	All	All	All
Hardware	Arm	Cortex-x1	-	All	All	All
Operating System	Arm	Cortex-x1 Firmware	-	All	All	All
Hardware	Arm	Cortex-x2	-	All	All	All
Operating System	Arm	Cortex-x2 Firmware	-	All	All	All
Hardware	Arm	Neoverse-e1	-	All	All	All
Operating System	Arm	Neoverse-e1 Firmware	-	All	All	All
Hardware	Arm	Neoverse-v1	-	All	All	All
Operating System	Arm	Neoverse-v1 Firmware	-	All	All	All
Hardware	Arm	Neoverse N1	-	All	All	All
Operating System	Arm	Neoverse N1 Firmware	-	All	All	All
Hardware	Arm	Neoverse N2	-	All	All	All
Operating System	Arm	Neoverse N2 Firmware	-	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Xen	Xen	-	All	All	All

References

Reference	Source	Link	Tags
Arm Security Center	MISC	developer.arm.com	
Debian -- Security Information -- DSA-5173-1 linux	DEBIAN	www.debian.org	
oss-security - Xen Security Advisory 398 v2 - Multiple speculative security issues	MLIST	www.openwall.com	
[SECURITY] [DLA 3065-1] linux security update	MLIST	lists.debian.org	
Speculative Processor Vulnerability – Arm Developer	CONFIRM	developer.arm.com	
CVE Program record	CVE.ORG	www.cve.org	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159727](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9245)

[159729](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9244)

[159754](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9274)

[159755](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9273)

[160210](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2022-7683)

[179221](#) Debian Security Update for linux (CVE-2022-23960)

[180282](#) Debian Security Update for linux (DLA 3065-1)

[180605](#) Debian Security Update for linux (DSA 5173-1)

[198694](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5317-1)

[198695](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5318-1)

[198728](#) Ubuntu Security Notification for Linux kernel (Intel IOTG) Vulnerabilities (USN-5362-1)

[240817](#) Red Hat Update for kernel security (RHSA-2022:7683)

[242941](#) Red Hat Update for kernel (RHSA-2024:0930)

[354279](#) Amazon Linux Security Advisory for kernel : ALAS2022-2022-039

[354468](#) Amazon Linux Security Advisory for kernel : ALAS2022-2022-185

[354542](#) Amazon Linux Security Advisory for kernel : ALAS-2022-185

[355199](#) Amazon Linux Security Advisory for kernel : ALAS2023-2023-070

[376925](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0125)

[378043](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0011)

[500806](#) Alpine Linux Security Update for xen

[610452](#) Google Android Devices December 2022 Security Patch Missing

[610462](#) Google Android Devices January 2023 Security Patch Missing

[610463](#) Google Android January 2023 Security Patch Missing for Samsung

[610467](#) Google Android February 2023 Security Patch Missing for Samsung

[671870](#) EulerOS Security Update for kernel (EulerOS-SA-2022-1934)

671915 EulerOS Security Update for kernel (EulerOS-SA-2022-1969)
671975 EulerOS Security Update for kernel (EulerOS-SA-2022-2159)
752039 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1196-1)
752120 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1651-1)
940732 AlmaLinux Security Update for kernel (ALSA-2022:7683)
960184 Rocky Linux Security Update for kernel (RLSA-2022:7683)

© [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](#)