CVE-2022-48251

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-48251
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-10 07:15:00 UTC
Updated	2023-11-07 03:56:00 UTC
Description	** DISPUTED ** The AES instructions on the ARMv8 platform do not have an algorithm that is "intrinsically resistant" to side

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Arm	Cortex-a53	-	All	All	All
Operating System	Arm	Cortex-a53 Firmware	-	All	All	All
Hardware	Arm	Cortex-a55	-	All	All	All
Operating System	Arm	Cortex-a55 Firmware	-	All	All	All
Hardware	Arm	Cortex-a57	-	All	All	All
Operating System	Arm	Cortex-a57 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
Operating System	Arm	Cortex-a78 Firmware	-	All	All	All

References

Reference	Source	Link	Tags
Apple vs. EMA: Electromagnetic Side Channel Attacks on Apple CoreCrypto	MISC	eprint.iacr.org	
404: This page could not be found	MISC	eshard.com	
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.

There are currently no legacy QID mappings associated with this CVE.