



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.

© [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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report