



CVE-2020-36423

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2020-36423 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-07-19 17:15:00 UTC |
| Updated | 2023-01-11 17:02:00 UTC |
| Description | An issue was discovered in Arm Mbed TLS before 2.23.0. A remote attacker can recover plaintext because a certain Lucky |

Risk And Classification

Problem Types: CWE-319

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|------------------------|------------------------------|---------|--------|---------|----------|
| Application | Arm | Mbed Tls | All | All | All | All |
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |

References

Reference

- [Release Mbed TLS 2.23.0 · ARMmbed/mbedtls · GitHub](#)
- [730752 – \(CVE-2020-36421, CVE-2020-36422, CVE-2020-36423\) <net-libs/mbedtls-{2.16.7,2.23.0}>: Multiple vulnerabilities \(CVE-2020-{3642](#)
- [Release Mbed TLS 2.16.7 · ARMmbed/mbedtls · GitHub](#)
- [\[SECURITY\] \[DLA 3249-1\] mbedtls security update](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[180642](#) Debian Security Update for mbedtls (CVE-2020-36423)

[181446](#) Debian Security Update for mbedtls (DLA 3249-1)

© [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](#)