



CVE-2019-18222

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2019-18222 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-01-23 17:15:00 UTC |
| Updated | 2023-03-03 15:25:00 UTC |
| Description | The ECDSA signature implementation in ecdsa.c in Arm Mbed Crypto 2.1 and Mbed TLS through 2.19.1 does not reduce th |

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|------------------------------|---------|--------|---------|----------|
| Application | Arm | Mbed Crypto | All | All | All | All |
| Application | Arm | Mbed Crypto | All | All | All | All |
| Application | Arm | Mbed Tls | All | All | All | All |
| Application | Arm | Mbed Tls | All | All | All | All |
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Operating System | Fedoraproject | Fedora | 30 | All | All | All |
| Operating System | Fedoraproject | Fedora | 31 | All | All | All |

References

| Reference | Source | Link | Tags |
|--|---------|---|----------|
| [SECURITY] Fedora 31 Update: mbedtls-2.16.4-1.fc31 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org | |
| [SECURITY] Fedora 31 Update: mbedtls-2.16.4-1.fc31 - package-announce - Fedora Mailing-Lists | MISC | lists.fedoraproject.org | |
| Security Advisories - Tech Updates - mbed TLS (Previously PolarSSL) | MISC | tls.mbed.org | Verified |
| [SECURITY] [DLA 3249-1] mbedtls security update | MLIST | lists.debian.org | |
| Side channel attack on ECDSA - Tech Updates - Mbed TLS (Previously PolarSSL) | CONFIRM | tls.mbed.org | Verified |
| [SECURITY] Fedora 30 Update: mbedtls-2.16.4-1.fc30 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org | |
| [SECURITY] Fedora 30 Update: mbedtls-2.16.4-1.fc30 - package-announce - Fedora Mailing-Lists | MISC | lists.fedoraproject.org | |

| | | | |
|--------------------------|---------|--|-----|
| CVE Program record | CVE.ORG | www.cve.org | car |
| NVD vulnerability detail | NVD | nvd.nist.gov | car |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|--|
| 181446 Debian Security Update for mbedtls (DLA 3249-1) |
| 500396 Alpine Linux Security Update for mbedtls |
| 504154 Alpine Linux Security Update for mbedtls |

© [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](#)