



CVE-2020-16150

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

Summary

CVE	CVE-2020-16150
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-02 16:15:00 UTC
Updated	2023-02-27 18:03:00 UTC
Description	A Lucky 13 timing side channel in mbedtls_ssl_decrypt_buf in library/ssl_msg.c in Trusted Firmware Mbed TLS through 2.2

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All

References

Reference	Source	Link
Local side channel attack on classical CBC decryption in (D)TLS - Tech Updates - Mbed TLS (Previously PolarSSL)	CONFIRM	tls.mbed.c
[SECURITY] Fedora 31 Update: mbedtls-2.16.8-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedor
[SECURITY] Fedora 32 Update: mbedtls-2.16.8-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedor
[SECURITY] Fedora 31 Update: mbedtls-2.16.8-1.fc31 - package-announce - Fedora Mailing-Lists	MISC	lists.fedor
[SECURITY] Fedora 32 Update: mbedtls-2.16.8-1.fc32 - package-announce - Fedora Mailing-Lists	MISC	lists.fedor
[SECURITY] Fedora 33 Update: mbedtls-2.16.8-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedor
Security Advisories - Tech Updates - mbed TLS (Previously PolarSSL)	MISC	tls.mbed.c
[SECURITY] [DLA 3249-1] mbedtls security update	MLIST	lists.debie

[SECURITY] Fedora 33 Update: mbedtls-2.16.8-1.fc33 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

[500398](#) Alpine Linux Security Update for mbedtls

[504156](#) Alpine Linux Security Update for mbedtls

[690500](#) Free Berkeley Software Distribution (FreeBSD) Security Update for mbed Transport Layer Security (TLS) (4c69240f-f02c-11ea-838a-0011d823eebd)

[710702](#) Gentoo Linux Mbed Transport Layer Security (TLS) Multiple Vulnerabilities (GLSA 202301-08)

© [CVE.report](https://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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org/). This site includes MITRE data granted under the following [license](#).

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