CVE-2020-16150

MITRE | NVD | CVE.ORG | Print: PDF

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.(
[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.(
[SECURITY] [DLA 3249-1] mbedtls security update	MLIST	lists.debia

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

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)