CVE-2020-10941

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-10941
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-24 20:15:00 UTC
Updated	2023-02-24 00:10:00 UTC
Description	Arm Mbed TLS before 2.16.5 allows attackers to obtain sensitive information (an RSA private key) by measuring cache usa

Risk And Classification

Problem Types: NVD-CWE-noinfo

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	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All

References

Reference	Source	Link	Tag
[SECURITY] Fedora 31 Update: mbedtls-2.16.7-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 32 Update: mbedtls-2.16.7-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 32 Update: mbedtls-2.16.7-1.fc32 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org	
Cache attack against RSA key import in SGX - Tech Updates - Mbed TLS (Previously PolarSSL)	MISC	tls.mbed.org	Ver
[SECURITY] Fedora 31 Update: mbedtls-2.16.7-1.fc31 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org	
[SECURITY] [DLA 3249-1] mbedtls security update	MLIST	lists.debian.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)