CVE-2021-45451

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-45451
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-21 07:15:00 UTC
Updated	2023-11-07 03:39:00 UTC
Description	In Mbed TLS before 3.1.0, psa_aead_generate_nonce allows policy bypass or oracle-based decryption when the output bu

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arm	Mbed Tls	All	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All

References

Reference	Source	Link	Tag
Release Mbed TLS 3.1.0 · ARMmbed/mbedtls · GitHub	MISC	github.com	
[SECURITY] Fedora 37 Update: mbedtls-2.28.1-1.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 36 Update: mbedtls-2.28.1-1.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 37 Update: mbedtls-2.28.1-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 36 Update: mbedtls-2.28.1-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	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

283264 Fedora Security Update for mbedtls (FEDORA-2022-ff582c5b0d)

283459 Fedora Security Update for mbedtls (FEDORA-2022-1dd9dc5140)