



# CVE-2021-45451

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-45451
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-12-21 07:15:00 UTC
<b>Updated</b>	2023-11-07 03:39:00 UTC
<b>Description</b>	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	<a href="#">Arm</a>	<a href="#">Mbed Tls</a>	All	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All

## References

Reference	Source	Link	Tag
Release Mbed TLS 3.1.0 · ARMmbed/mbedtls · GitHub	MISC	<a href="#">github.com</a>	
[SECURITY] Fedora 37 Update: mbedtls-2.28.1-1.fc37 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>	
[SECURITY] Fedora 36 Update: mbedtls-2.28.1-1.fc36 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>	
[SECURITY] Fedora 37 Update: mbedtls-2.28.1-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>	
[SECURITY] Fedora 36 Update: mbedtls-2.28.1-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	car
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	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)

© [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](#)