



CVE-2021-43085

Published on: Not Yet Published

Last Modified on: 03/30/2022 02:15:00 PM UTC

CVE-2021-43085

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

The following vulnerability was found:

**** REJECT ** DO NOT USE THIS CANDIDATE NUMBER.** ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.

CVE-2021-43085 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVE References

Description	Tags	Link
CMAC encryption result error caused by wrong implementation of CMAC_Final() · Issue #16873 · openssl/openssl · GitHub	github.com text/html	MISC github.com/openssl/openssl/issues/16873

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

There are no known software configurations (CPEs) currently associated with this CVE

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-43085 : An Insecure Permissions vulnerability exists in the OpenSSL Project 3.0 due to an error in the imp... twitter.com/i/web/status/1...	2022-03-24 18:05:50
/r/netcve	CVE-2021-43085	2022-03-24 19:38:43

[Previous ID](#)[Next ID](#)

© [CVE.report](#) 2023   |

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](#)