



CVE-2023-4807

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

Summary

CVE	CVE-2023-4807
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-08 12:15:00 UTC
Updated	2023-09-21 17:15:00 UTC
Description	Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	All	All	All	All

References

Reference	Source	Link	Tags
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org	
OpenSSL Security Advisory 20230908 ~ Packet Storm	MISC	packetstormsecurity.com	
CVE-2023-4807 OpenSSL Vulnerability in NetApp Products NetApp Product Security	MISC	security.netapp.com	
www.openssl.org/news/secadv/20230908.txt	MISC	www.openssl.org	
oss-security - OpenSSL Security Advisory	MISC	www.openwall.com	
oss-security - Re: OpenSSL Security Advisory	MISC	www.openwall.com	
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org	
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, e

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

673599 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-3283)

673869 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-3255)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)