



# CVE-2023-6129

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

## Summary

<b>CVE</b>	CVE-2023-6129
<b>State</b>	PUBLISHED
<b>Assigner</b>	Unknown
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-01-09 17:15:00 UTC
<b>Updated</b>	2024-01-23 21:32:00 UTC
<b>Description</b>	Description unavailable.

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	3.2.0	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	All	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	All	All	All	All

## References

Reference	Source	Link	Tags
poly1305-ppc.pl: Fix vector register clobbering · openssl/openssl@5b139f9 · GitHub		<a href="#">github.com</a>	Patch
poly1305-ppc.pl: Fix vector register clobbering · openssl/openssl@f3fc580 · GitHub		<a href="#">github.com</a>	Patch
OpenSSL Advisory		<a href="#">www.openssl.org</a>	Vendor Advisory
poly1305-ppc.pl: Fix vector register clobbering · openssl/openssl@050d263 · GitHub		<a href="#">github.com</a>	Patch
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[200094](#) Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-6622-1)

[330164](#) IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (openssl\_advisory40)

[CVE-2023-38861](#) IBM Advanced Interactive Executive (AIX) Open Secure Sockets Layer (OpenSSL) multiple vulnerabilities (openssl\_advisory70)

[505912](#) Alpine Linux Security Update for openssl

[506285](#) Alpine Linux Security Update for openssl

[520013](#) Open Secure Sockets Layer (OpenSSL) POLY1305 MAC Improper Authentication (CVE-2023-6129)

[691394](#) Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (8337251b-b07b-11ee-b0d7-84a93843eb75)

[755637](#) SUSE Enterprise Linux Security Update for openssl-3 (SUSE-SU-2024:0172-1)

[755771](#) SUSE Enterprise Linux Security Update for openssl-3 (SUSE-SU-2024:0518-1)

© [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](#)