CVE-2023-6129

MITRE | NVD | CVE.ORG | Print: PDF

Summary

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

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	3.2.0	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	All	All	All	All

References

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

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)