CVE-2023-2975

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-2975
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-14 12:15:00 UTC
Updated	2024-02-04 09:15:00 UTC
Description	Issue summary: The AES-SIV cipher implementation contains a bug that causes it to ignore empty associated data entries

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Management Services For Element Software And Netapp Hci	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	All	All	All	All

References

Reference	Source	Link	Tags
oss-security - OpenSSL Security Advisory	MISC	www.openwall.com	
OpenSSL: Multiple Vulnerabilities (GLSA 202402-08) — Gentoo security		security.gentoo.org	
git.openssl.org Git - openssl.git/commitdiff	MISC	git.openssl.org	
/err404.html	MISC	www.openssl.org	
oss-security - Re: OpenSSL Security Advisory	MISC	www.openwall.com	
CVE-2023-2975 OpenSSL Vulnerability in NetApp Products | NetApp Product Security	MISC	security.netapp.com	
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, analys

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

199860 Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-6450-1)

296105 Oracle Solaris 11.4 Support Repository Update (SRU) 63.157.1 Missing (CPUOCT2023)

330149 IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (openssl_advisory39)

355881 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-306

503039 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)3

503040 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

503122 Alpine Linux Security Update for openssl

505907 Alpine Linux Security Update for openssl

691212 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (41c60e16-2405-11ee-a0d1-84a93843eb75)

710857 Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 202402-08)