Potential Use-after-free in DANE Client Code

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-28387
State	PUBLISHED
Assigner	openssl
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 22:16:20 UTC
Updated	2026-04-23 15:39:25 UTC
Description	Issue summary: An uncommon configuration of clients performing DANE TLSA-based server authentication, when paired w

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000210000 probability, percentile 0.055150000 (date 2026-04-14)

Problem Types: CWE-416 | CWE-416 CWE-416 Use After Free

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OpenSSL	OpenSSL	affected 3.6.0 3.6.2 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.5.0 3.5.6 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.4.0 3.4.5 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.3.0 3.3.7 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.0.0 3.0.20 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 1.1.1 1.1.1zg custom	Not specified

References

Reference	Source	Link
github.com/openssl/openssl/commit/7a4e08cee62a728d32e60b0de89e6764339df0a7	openssl-security@openssl.org	github.com
github.com/openssl/openssl/commit/07e727d304746edb49a98ee8f6ab00256e1f012b	openssl-security@openssl.org	github.com
openssl-library.org/news/secadv/20260407.txt	openssl-security@openssl.org	openssl-library.org
github.com/openssl/openssl/commit/258a8f63b26995ba357f4326da00e19e29c6acbe	openssl-security@openssl.org	github.com
github.com/openssl/openssl/commit/444958deaf450aea819171f97ae69eaedede42c3	openssl-security@openssl.org	github.com
github.com/openssl/openssl/commit/ec03fa050b3346997ed9c5fef3d0e16ad7db8177	openssl-security@openssl.org	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Igor Morgenstern (Aisle Research) (en)

CNA: Viktor Dukhovni (en)

CNA: Alexandr Nedvedicky (en)

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report