OpenSSL TLS 1.3 server may choose unexpected key agreement group

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

Summary

CVE	CVE-2026-2673
State	PUBLISHED
Assigner	openssl
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-13 19:54:34 UTC
Updated	2026-05-12 13:17:34 UTC
Description	Issue summary: An OpenSSL TLS 1.3 server may fail to negotiate the expected preferred key exchange group when its key

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from ADP

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

EPSS: 0.000170000 probability, percentile 0.045070000 (date 2026-05-12)

Problem Types: CWE-757 | CWE-757 CWE-757 Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

None

Availability

None

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

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
ADP	Siemens	SIMATIC CN 4100	affected V5.0 custom	Not specified

References

Reference	Source	Link
github.com/openssl/openssl/commit/2157c9d81f7b0bd7dfa25b960e928ec28e8dd63f	openssl-security@openssl.org	github.c
cert-portal.siemens.com/productcert/html/ssa-032379.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-port
github.com/openssl/openssl/commit/85977e013f32ceb96aa034c0e741adddc1a05e34	openssl-security@openssl.org	github.c
openssl-library.org/news/secadv/20260313.txt	openssl-security@openssl.org	openssl-
www.openwall.com/lists/oss-security/2026/03/13/3	af854a3a-2127-422b-91ae-364da2661108	www.op
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist.

Vendor Comments And Credit

Discovery Credit

CNA: Viktor Dukhovni (en)

CNA: Viktor Dukhovni (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**