Unauthenticated/unencrypted trailing bytes with low-level OCB function calls

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

Summary

CVE	CVE-2025-69418
State	PUBLISHED
Assigner	openssl
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-27 16:16:33 UTC
Updated	2026-05-12 13:17:24 UTC
Description	Issue summary: When using the low-level OCB API directly with AES-NI or other hardware-accelerated code paths, inp

Risk And Classification

Primary CVSS: v3.1 4 MEDIUM from ADP

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

Problem Types: CWE-325 | CWE-325 CWE-325 Missing Cryptographic Step

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

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
High

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
Low

Integrity
Low

Availability

None

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

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 3.6.1 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.5.0 3.5.5 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.4.0 3.4.4 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.3.0 3.3.6 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.0.0 3.0.19 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 1.1.1 1.1.1ze custom	Not specified
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom	Not specified

References

Reference	Source	Link
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-porta
github.com/openssl/openssl/commit/ed40856d7d4ba6cb42779b6770666a65f19cb977	openssl-security@openssl.org	github.co
github.com/openssl/openssl/commit/372fc5c77529695b05b4f5b5187691a57ef5dffc	openssl-security@openssl.org	github.co
openssl-library.org/news/secadv/20260127.txt	openssl-security@openssl.org	openssl-li
github.com/openssl/openssl/commit/a7589230356d908c0eca4b969ec4f62106f4f5ae	openssl-security@openssl.org	github.co
github.com/openssl/openssl/commit/52d23c86a54adab5ee9f80e48b242b52c4cc2347	openssl-security@openssl.org	github.co
github.com/openssl/openssl/commit/4016975d4469cd6b94927c607f7c511385f928d8	openssl-security@openssl.org	github.co
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

CNA: Stanislav Fort (Aisle Research) (en)

CNA: Stanislav Fort (Aisle Research) (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**