Missing ASN1_TYPE validation in TS_RESP_verify_response() function

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

Summary

CVE	CVE-2025-69420
State	PUBLISHED
Assigner	openssl
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-27 16:16:34 UTC
Updated	2026-05-12 13:17:26 UTC
Description	Issue summary: A type confusion vulnerability exists in the TimeStamp Response verification code where an ASN1_TYPE

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:N/I:N/A:H

Problem Types: CWE-754 | CWE-754 CWE-754 Improper Check for Unusual or Exceptional Conditions

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:N/I:N/A:H
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:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/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 3.6.1 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
github.com/openssl/openssl/commit/a99349ebfc519999edc50620abe24d599b9eb085	openssl-security@openssl.org	github.co
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-porta
github.com/openssl/openssl/commit/4e254b48ad93cc092be3dd62d97015f33f73133a	openssl-security@openssl.org	github.co
openssl-library.org/news/secadv/20260127.txt	openssl-security@openssl.org	openssl-li
github.com/openssl/openssl/commit/27c7012c91cc986a598d7540f3079dfde2416eb9	openssl-security@openssl.org	github.co
github.com/openssl/openssl/commit/5eb0770ffcf11b785cf374ff3c19196245e54f1b	openssl-security@openssl.org	github.co
github.com/openssl/openssl/commit/564fd9c73787f25693bf9e75faf7bf6bb1305d4e	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: Luigino Camastra (Aisle Research) (en)

CNA: Bob Beck (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**