



# Missing ASN1\_TYPE validation in TS\_RESP\_verify\_response() function

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2025-69420
<b>State</b>	PUBLISHED
<b>Assigner</b>	openssl
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-01-27 16:16:34 UTC
<b>Updated</b>	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	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 3.6.0 3.6.1 semver	Not specified
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 3.5.0 3.5.5 semver	Not specified
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 3.4.0 3.4.4 semver	Not specified
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 3.3.0 3.3.6 semver	Not specified
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 3.0.0 3.0.19 semver	Not specified
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 1.1.1 1.1.1ze custom	Not specified
ADP	<a href="#">Siemens</a>	<a href="#">SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem</a>	affected * custom	Not specified

### References

Reference	Source	Link
<a href="https://github.com/openssl/openssl/commit/a99349ebfc519999edc50620abe24d599b9eb085">github.com/openssl/openssl/commit/a99349ebfc519999edc50620abe24d599b9eb085</a>	<a href="mailto:openssl-security@openssl.org">openssl-security@openssl.org</a>	<a href="#">github.co</a>
<a href="https://cert-portal.siemens.com/productcert/html/ssa-265688.html">cert-portal.siemens.com/productcert/html/ssa-265688.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="#">cert-porta</a>
<a href="https://github.com/openssl/openssl/commit/4e254b48ad93cc092be3dd62d97015f33f73133a">github.com/openssl/openssl/commit/4e254b48ad93cc092be3dd62d97015f33f73133a</a>	<a href="mailto:openssl-security@openssl.org">openssl-security@openssl.org</a>	<a href="#">github.co</a>
<a href="https://openssl-library.org/news/secadv/20260127.txt">openssl-library.org/news/secadv/20260127.txt</a>	<a href="mailto:openssl-security@openssl.org">openssl-security@openssl.org</a>	<a href="#">openssl-li</a>
<a href="https://github.com/openssl/openssl/commit/27c7012c91cc986a598d7540f3079dfde2416eb9">github.com/openssl/openssl/commit/27c7012c91cc986a598d7540f3079dfde2416eb9</a>	<a href="mailto:openssl-security@openssl.org">openssl-security@openssl.org</a>	<a href="#">github.co</a>
<a href="https://github.com/openssl/openssl/commit/5eb0770ffc11b785cf374ff3c19196245e54f1b">github.com/openssl/openssl/commit/5eb0770ffc11b785cf374ff3c19196245e54f1b</a>	<a href="mailto:openssl-security@openssl.org">openssl-security@openssl.org</a>	<a href="#">github.co</a>
<a href="https://github.com/openssl/openssl/commit/564fd9c73787f25693bf9e75faf7bf6bb1305d4e">github.com/openssl/openssl/commit/564fd9c73787f25693bf9e75faf7bf6bb1305d4e</a>	<a href="mailto:openssl-security@openssl.org">openssl-security@openssl.org</a>	<a href="#">github.co</a>
CVE Program record	CVE.ORG	<a href="http://www.cve">www.cve.</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.g">nvd.nist.g</a>

### 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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)