ASN1_TYPE Type Confusion in the PKCS7_digest_from_attributes() function

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

Summary

CVE	CVE-2026-22796
State	PUBLISHED
Assigner	openssl
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-27 16:16:35 UTC
Updated	2026-05-12 13:17:32 UTC
Description	Issue summary: A type confusion vulnerability exists in the signature verification of signed PKCS#7 data where an ASN1_T

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from ADP

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

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	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

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

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
CNA	OpenSSL	OpenSSL	affected 1.0.2 1.0.2zn 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/eeee3cbd4d682095ed431052f00403004596373e	openssl-security@openssl.org	github.co
github.com/openssl/openssl/commit/7bbca05be55b129651d9df4bdb92becc45002c12	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/2502e7b7d4c0cf4f972a881641fe09edc67aeec4	openssl-security@openssl.org	github.co
openssl-library.org/news/secadv/20260127.txt	openssl-security@openssl.org	openssl-li
github.com/openssl/openssl/commit/572844beca95068394c916626a6d3a490f831a49	openssl-security@openssl.org	github.co
github.com/openssl/openssl/commit/ef2fb66ec571564d64d1c74a12e388a2a54d05d2	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: Rob Rock (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**