Incorrect Failure Handling in RSA KEM RSASVE Encapsulation

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

Summary

CVE	CVE-2026-31790
State	PUBLISHED
Assigner	openssl
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 22:16:21 UTC
Updated	2026-04-08 21:27:00 UTC
Description	Issue summary: Applications using RSASVE key encapsulation to establish a secret encryption key can send contents of a

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: 0.000240000 probability, percentile 0.062830000 (date 2026-04-14)

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: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
CNA	OpenSSL	OpenSSL	affected 3.4.0 3.4.5 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.3.0 3.3.7 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.0.0 3.0.20 semver	Not specified

References

Reference	Source	Link
github.com/openssl/openssl/commit/eed200f58cd8645ed77e46b7e9f764e284df379e	openssl-security@openssl.org	github.com
openssl-library.org/news/secadv/20260407.txt	openssl-security@openssl.org	openssl-library.org
github.com/openssl/openssl/commit/001e01db3e996e13ffc72386fe79d03a6683b5ac	openssl-security@openssl.org	github.com
github.com/openssl/openssl/commit/b922e24e5b23ffb9cb9e14cadff23d91e9f7e406	openssl-security@openssl.org	github.com
github.com/openssl/openssl/commit/d5f8e71cd0a54e961d0c3b174348f8308486f790	openssl-security@openssl.org	github.com
github.com/openssl/openssl/commit/abd8b2eec7e3f3fda60ecfb68498b246b52af482	openssl-security@openssl.org	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Simo Sorce (Red Hat) (en)

CNA: Nikola Pajkovsky (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