LibJWT has NULL/bounds validation in JWK octet and RSA PSS parsing

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-33996
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 23:17:14 UTC
Updated	2026-03-31 20:39:06 UTC
Description	LibJWT is a C JSON Web Token Library. Starting in version 3.0.0 and prior to version 3.3.0, the JWK parsing for RSA-PSS

Risk And Classification

Primary CVSS: v4.0 5.8 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:A/AC:H/AT:P/PR:N/UI:A/VC:L/VI:L/VA:H/SC:L/SI:L/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000140000 probability, percentile 0.022580000 (date 2026-04-01)

Problem Types: CWE-476 | CWE-476 CWE-476: NULL Pointer Dereference

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	5.8	MEDIUM	CVSS:4.0/AV:A/AC:H/AT:P/PR:N/UI:A/VC:L/VI:L/VA:H/SC:L/S
4.0	CNA	DECLARED	5.8	MEDIUM	CVSS:4.0/AV:A/AC:H/AT:P/PR:N/UI:A/VC:L/VI:L/VA:H/SC:L/S
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

High

Attack Requirements

Present

Privileges Required

None

User Interaction

Active

Confidentiality

Low

Integrity

Low

Availability

High

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

Low

CVSS:4.0/AV:A/AC:H/AT:P/PR:N/UI:A/VC:L/VI:L/VA:H/SC:L/SI:L/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libjwt	Libjwt	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms

CNA	Benmcollins	Libjwt	affected >= 3.0.0, < 3.3.0	Not specified

References

Reference	Source	Link	Tags
github.com/benmcollins/libjwt/security/advisories/GHSA-ph96-hqpc-9f66	security-advisories@github.com	github.com	Mitigati
github.com/benmcollins/libjwt/commit/cfd890286fa49ae61b534c937c9f0428b5c...	security-advisories@github.com	github.com	Patch
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.