quickjs-ng quickjs quickjs.c js_typed_array_constructor heap-based overflow

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

Summary

CVE	CVE-2026-0821
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-10 13:15:49 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability was determined in quickjs-ng quickjs up to 0.11.0. This vulnerability affects the function js_typed_array_cons

Risk And Classification

Primary CVSS: v4.0 5.5 MEDIUM from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/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

Problem Types: CWE-119 | CWE-122 | CWE-122 Heap-based Buffer Overflow | CWE-119 Memory Corruption

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	5.5	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C.
4.0	CNA	DECLARED	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	cna@vuldb.com	Secondary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
3.0	CNA	DECLARED	7.3	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P
2.0	CNA	DECLARED	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/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

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Quickjs-ng	Quickjs	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Quickjs-ng	Quickjs	affected 0.1	Not specified
CNA	Quickjs-ng	Quickjs	affected 0.2	Not specified
CNA	Quickjs-ng	Quickjs	affected 0.3	Not specified
CNA	Quickjs-ng	Quickjs	affected 0.4	Not specified
CNA	Quickjs-ng	Quickjs	affected 0.5	Not specified
CNA	Quickjs-ng	Quickjs	affected 0.6	Not specified
CNA	Quickjs-ng	Quickjs	affected 0.7	Not specified
CNA	Quickjs-ng	Quickjs	affected 0.8	Not specified
CNA	Quickjs-ng	Quickjs	affected 0.9	Not specified
CNA	Quickjs-ng	Quickjs	affected 0.10	Not specified
CNA	Quickjs-ng	Quickjs	affected 0.11.0	Not specified

References

Reference	Source	Link	Tags
vuldb.com	cna@vuldb.com	vuldb.com	Permissions Required
github.com/quickjs-ng/quickjs/commit/c5d80831e51e48a83eab16ea867be87f091	cna@vuldb.com	github.com	Patch

github.com/quickjs-ng/quickjs/issues/1296	cna@vuldb.com	github.com	Exploit, Issue Tracking
github.com/quickjs-ng/quickjs/pull/1299	cna@vuldb.com	github.com	Issue Tracking
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advisory,
github.com/quickjs-ng/quickjs	cna@vuldb.com	github.com	
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advisory,
github.com/quickjs-ng/quickjs/issues/1296	cna@vuldb.com	github.com	Exploit, Issue Tracking
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: mcsky23 (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-01-09T00:00:00.000Z	Advisory disclosed
CNA	2026-01-09T01:00:00.000Z	VulDB entry created
CNA	2026-01-16T01:25:36.000Z	VulDB entry last update

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