A stack overflow and DoS vulnerability in DTStack/chunjun

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

Summary

CVE	CVE-2026-4735
State	PUBLISHED
Assigner	GovTech CSG
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-24 04:17:26 UTC
Updated	2026-04-30 16:01:57 UTC
Description	Deserialization of Untrusted Data vulnerability in DTStack chunjun (chunjun-core/src/main/java/com/dtstack/chunjun/util mo

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from cve_disclosure@tech.gov.sg

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H/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:N/AU:Y/R:U/V:C/RE:M/U:Amber

EPSS: 0.000570000 probability, percentile 0.176520000 (date 2026-05-05)

Problem Types: CWE-502 | CWE-502 CWE-502 Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
4.0	cve_disclosure@tech.gov.sg	Secondary	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/S
4.0	CNA	CVSS	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H/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:N/AU:Y/R:U/V:C/RE:M/U:Amber

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	DTStack	Chunjun	affected 1.16.1 git	Not specified

References

Reference	Source	Link	Tags
github.com/DTStack/chunjun/pull/1939	cve_disclosure@tech.gov.sg	github.com	
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: TITAN Team (titancaproject@gmail.com) (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**