



Hot Chocolate's Utf8GraphQLParser has Stack Overflow via Deeply Nested GraphQL Documents

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-40324
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-18 00:16:36 UTC
Updated	2026-04-18 00:16:36 UTC

Description Hot Chocolate is an open-source GraphQL server. Prior to versions 12.22.7, 13.9.16, 14.3.1, and 15.1.14, Hot Chocolate's

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from security-advisories@github.com

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

Problem Types: CWE-674 | CWE-674 CWE-674: Uncontrolled Recursion

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
3.1	CNA	DECLARED	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ChilliCream	GraphQL-platform	affected < 12.22.7	Not specified
CNA	ChilliCream	GraphQL-platform	affected >= 13.0.0, < 13.9.16	Not specified
CNA	ChilliCream	GraphQL-platform	affected >= 14.0.0, < 14.3.1	Not specified
CNA	ChilliCream	GraphQL-platform	affected >= 15.0.0, < 15.1.14	Not specified

References

Reference	Source	Link	Tags
github.com/ChilliCream/graphql-platform/commit/b185eb276c9ee227bd44616ff...	security-advisories@github.com	github.com	
github.com/ChilliCream/graphql-platform/commit/b9271e6a500484c002fd528dc...	security-advisories@github.com	github.com	
github.com/ChilliCream/graphql-platform/pull/9531	security-advisories@github.com	github.com	
github.com/ChilliCream/graphql-platform/pull/9528	security-advisories@github.com	github.com	
github.com/ChilliCream/graphql-platform/releases/tag/15.1.14	security-advisories@github.com	github.com	
github.com/ChilliCream/graphql-platform/commit/4cbaf67d366f800fc1e484bc5...	security-advisories@github.com	github.com	
github.com/ChilliCream/graphql-platform/releases/tag/14.3.1	security-advisories@github.com	github.com	
github.com/ChilliCream/graphql-platform/releases/tag/12.22.7	security-advisories@github.com	github.com	
github.com/ChilliCream/graphql-platform/commit/08c0caa42ca33c121bbed49d2...	security-advisories@github.com	github.com	
github.com/ChilliCream/graphql-platform/pull/9530	security-advisories@github.com	github.com	
github.com/ChilliCream/graphql-platform/releases/tag/13.9.16	security-advisories@github.com	github.com	
github.com/ChilliCream/graphql-platform/security/advisories/GHSA-qr3m-xw...	security-advisories@github.com	github.com	
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.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report