Utf8GraphQLParser Stack Overflow via Deeply Nested GraphQL Documents

Critical **michaelstaib** published **GHSA-qr3m-xw4c-jqw3** yesterday

Package

HotChocolate.Language (NuGet)

Affected versions	Patched versions
< 15.1.14	15.1.14

Description

Impact

Hot Chocolate's `Utf8GraphQLParser` is a recursive descent parser with no recursion depth limit. A crafted GraphQL document with deeply nested selection sets, object values, list values, or list types can trigger a `StackOverflowException` on payloads as small as **40 KB**.

Because `StackOverflowException` is **uncatchable in .NET** (since .NET 2.0), the entire worker process is terminated immediately. All in-flight HTTP requests, background `IHostedService` tasks, and open WebSocket subscriptions on that worker are dropped. The orchestrator (Kubernetes, IIS, etc.) must restart the process.

This occurs **before any validation rules run** — `MaxExecutionDepth`, complexity analyzers, persisted query allow-lists, and custom `IDocumentValidatorRule` implementations cannot intercept the crash because `Utf8GraphQLParser.Parse` is invoked before validation. The existing `MaxAllowedFields=2048` limit does not help because the crashing payloads contain very few fields.

Severity: Critical (9.1) — `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H`

Patches

- **v12 line:** Fixed in `12.22.7`
- **v13 line:** Fixed in `13.9.16`
- **v14 line:** Fixed in `14.3.1`

- **v15 line:** Fixed in `15.1.14`

The fix adds a `MaxAllowedRecursionDepth` option to `ParserOptions` with a safe default, and enforces it across all recursive parser methods (`ParseSelectionSet`, `ParseValueLiteral`, `ParseObject`, `ParseList`, `ParseTypeReference`, etc.). When the limit is exceeded, a catchable `SyntaxException` is thrown instead of overflowing the stack.

Workarounds

There is no application-level workaround. `StackOverflowException` cannot be caught in .NET. The only mitigation is to upgrade to a patched version.

Operators can reduce (but not eliminate) risk by limiting HTTP request body size at the reverse proxy or load balancer layer, though the smallest crashing payload (40 KB) is well below most default body size limits and is highly compressible (~few hundred bytes via gzip).

References

- Fix for v15: #9528

Severity

Critical 9.1 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	High
Availability	High

Learn more about base metrics

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

CVE ID

CVE-2026-40324

Weaknesses

▶ CWE-674

Credits

BZHunt — Reporter