OneCollector exporter reads unbounded HTTP response bodies

Moderate **arminru** published **GHSA-55m9-299j-53c7** last week

Package

OpenTelemetry.Exporter.OneCollector (NuGet)

Affected versions	Patched versions
<= 1.15.0	1.15.1

Description

Summary

When exporting telemetry to a back-end/collector over HTTP using the OpenTelemetry.Exporter.OneCollector exporter, if the request results in a unsuccessful request (i.e. HTTP 4xx or 5xx), the response is read into memory with no upper-bound on the number of bytes consumed.

This could cause memory exhaustion in the consuming application if the configured back-end/collector endpoint is attacker-controlled (or a network attacker can MitM the connection) and an extremely large body is returned by the response.

Details

The `HttpJsonPostTransport` class reads the response body when a non-200 HTTP status code is received when exporting telemetry to aid debugging by operators so that the error response is included in the logs emitted by the exporter.

An attacker who controls the configured endpoint, or who can intercept traffic to them (MiTM), can return an arbitrarily large response body. This causes unbounded heap allocation in the consuming process, leading to high transient memory pressure, garbage-collection stalls, or an OutOfMemoryException that terminates the process.

Impact

If an application using the OneCollector exporter is configured to use a back-end/collector endpoint that is attacker-controlled (or a network attacker can MitM the connection) and an extremely large body is returned by the response the application could have its memory exhausted and create a denial-of-service condition.

Mitigation

The application's configured back-end/collector endpoint needs to behave maliciously. If the collector/back-end is a well-behaved implementation response bodies should not be excessively large if a request error occurs.

Workarounds

Use network-level controls (firewall rules, mTLS, service mesh) to prevent Man-in-the-Middle (MitM) attacks on the configured back-end/collector endpoint.

Remediation

#4117 updates the OneCollector exporter to limit the number of bytes read from the response body in an error condition to 4MiB.

References

- #4117

Severity

Moderate 5.3 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-41484

Weaknesses

▶ CWE-770

Credits

martincostello Remediation developer

rajkumar-rangaraj Remediation reviewer