Unbounded HTTP response body read in OpenTelemetry.Resources.Azure

Moderate **arminru** published **GHSA-vc24-j8c5-2vw4** last week

Package

OpenTelemetry.Resources.Azure (NuGet)

Affected versions	Patched versions
<= 1.15.0-beta.1	1.15.1-beta.1

Description

Summary

`OpenTelemetry.Resources.Azure` reads unbounded HTTP response bodies from the Azure VM remote instance metadata service endpoint into memory.

This would allow an attacker-controlled endpoint or one acting as a Man-in-the-Middle (MitM) to cause excessive memory allocation and possible process termination (via Out of Memory (OOM)).

Details

The `AzureVmMetaDataRequestor` class makes HTTP requests to the relevant Azure VM instance metadata service (`http://169.254.169.254`) to obtain metadata about the running process and its infrastructure.

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

Denial of Service (DoS). An attacker can destabilize or crash the application by forcing unbounded memory allocation through the Azure VM instance metadata HTTP response paths.

Mitigating Factors

The application's reachable Azure VM metadata endpoint needs to behave maliciously or be subject to MitM. In normal usage response bodies should not be excessively large.

Patches

Fixed in `OpenTelemetry.Resources.Azure` version `1.15.0-beta.2`.

The fix (#4121) introduce changes that introduce limits to `HttpClient` requests so that the response body is streamed rather than buffered entirely in memory. Responses greater than 4 MiB are ignored.

Workarounds

- Disable the Azure VM resource detector.
- Use network-level controls (firewall rules, mTLS, service mesh) to prevent Man-in-the-Middle (MitM) attacks on the Azure VM instance metadata endpoint.

References

- #4121

Severity

Moderate 5.9 / 10

CVSS v3 base metrics

Attack vector	Network
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:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE ID

CVE-2026-41483

Weaknesses

▶ CWE-770

Credits

martincostello Remediation developer

Kielek Remediation reviewer