

New issue

Jump to bottom

crash when udp packet size large than 1500 #14113

🔒 Closed 3ks opened this issue on Nov 20, 2020 · 4 comments · Fixed by #14122

Labels bug triage

3ks commented on Nov 20, 2020 • edited

Contributor

crash when udp packet size large than 1500

Description

envoy crash when udp packet size large than 1500.

Is there any way to change the udp packet size limit?

Repro steps

- start envoy
- envoy crash when receive packget that size larger than 1500

```
conf-jira-envoy | [2020-11-20 05:38:55.476][73][warning][misc] [source/common/network/io_socket_handle_impl.cc:395] Dropping truncated UDP packet with size: 1686.
conf-jira-envoy | [2020-11-20 05:38:55.476][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:104] Caught
Segmentation fault, suspect faulting address 0x0
conf-jira-envoy | [2020-11-20 05:38:55.476][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:91] Backtrace (use
tools/stack_decode.py to get line numbers):
conf-jira-envoy | [2020-11-20 05:38:55.476][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:92] Envoy version:
8fb3cb86082b17144a80402f5367ae65f06083bd/1.16.0/Clean/RELEASE/BoringSSL
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:96] #0: __restore_rt
[0x7f9c2d4138a0]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #1:
[0x5563a383b4ee]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #2:
[0x5563a383bd47]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #3:
[0x5563a3689030]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #4:
[0x5563a3688de1]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #5:
[0x5563a3414366]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #6:
[0x5563a384cfe8]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #7:
[0x5563a384b9be]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #8:
[0x5563a3405838]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #9:
[0x5563a39fa8c3]
conf-jira-envoy | [2020-11-20 05:38:55.478][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:96] #10: start_thread
[0x7f9c2d4086db]
conf-jira-envoy exited with code 139
```

Config


```
admin:
  access_log_path: /tmp/admin_access.log
  address:
    socket_address:
      protocol: TCP
      address: 0.0.0.0
      port_value: 9901
static_resources:
  listeners:
    - name: listener_udp
      reuse_port: true
      address:
        socket_address:
          protocol: UDP
          address: 0.0.0.0
          port_value: 5144
      listener_filters:
        name: envoy.filters.udp_listener.udp_proxy
      typed_config:
        '@type': type.googleapis.com/envoy.extensions.filters.udp.udp_proxy.v3.UdpProxyConfig
        stat_prefix: service
        cluster: conf_jira_udp
  clusters:
    - name: conf_jira_udp
      connect_timeout: 0.25s
      type: STATIC
      lb_policy: ROUND_ROBIN
      load_assignment:
        cluster_name: conf_jira_udp
        endpoints:
```

```
- lb_endpoints:
  - endpoint:
      address:
        socket_address:
          address: 172.16.10.10
          port_value: 6144
```

Logs

```
conf-jira-envoy | [2020-11-20 05:36:51.503][1][info][config] [source/server/configuration_impl.cc:95] loading tracing configuration
conf-jira-envoy | [2020-11-20 05:36:51.503][1][info][config] [source/server/configuration_impl.cc:70] loading 0 static secret(s)
conf-jira-envoy | [2020-11-20 05:36:51.503][1][info][config] [source/server/configuration_impl.cc:76] loading 1 cluster(s)
conf-jira-envoy | [2020-11-20 05:36:51.506][1][info][config] [source/server/configuration_impl.cc:80] loading 1 listener(s)
conf-jira-envoy | [2020-11-20 05:36:51.506][1][info][config] [source/server/configuration_impl.cc:121] loading stats sink configuration
conf-jira-envoy | [2020-11-20 05:36:51.506][1][info][runtime] [source/common/runtime/runtime_impl.cc:421] RTDS has finished initialization
conf-jira-envoy | [2020-11-20 05:36:51.506][1][info][upstream] [source/common/upstream/cluster_manager_impl.cc:178] cm init: all clusters initialized
conf-jira-envoy | [2020-11-20 05:36:51.506][1][warning][main] [source/server/server.cc:565] there is no configured limit to the number of allowed active connections. Set a limit
via the runtime key overload.global_downstream_max_connections
conf-jira-v2 | Nov 20 05:36:51.507 INFO vector::topology::builder: Healthcheck: Passed.
conf-jira-envoy | [2020-11-20 05:36:51.508][1][info][main] [source/server/server.cc:660] all clusters initialized. initializing init manager
conf-jira-envoy | [2020-11-20 05:36:51.508][1][info][config] [source/server/listener_manager_impl.cc:888] all dependencies initialized. starting workers
conf-jira-envoy | [2020-11-20 05:36:51.530][1][info][main] [source/server/server.cc:679] starting main dispatch loop

conf-jira-envoy | [2020-11-20 05:38:55.476][73][warning][misc] [source/common/network/io_socket_handle_impl.cc:395] Dropping truncated UDP packet with size: 1686.
conf-jira-envoy | [2020-11-20 05:38:55.476][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:104] Caught
Segmentation fault, suspect faulting address 0x0
conf-jira-envoy | [2020-11-20 05:38:55.476][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:91] Backtrace (use
tools/stack_decode.py to get line numbers):
conf-jira-envoy | [2020-11-20 05:38:55.476][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:92] Envoy version:
8fb3cb86082b17144a88402f5367ae65f06083bd/1.16.0/Clean/RELEASE/BoringSSL
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:96] #0: __restore_rt
[0x7f9c2d4138a0]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #1:
[0x5563a383b4ee]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #2:
[0x5563a383bd47]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #3:
[0x5563a3689030]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #4:
[0x5563a3688de1]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #5:
[0x5563a3414366]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #6:
[0x5563a384cfe8]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #7:
[0x5563a384b9be]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #8:
[0x5563a3405838]
conf-jira-envoy | [2020-11-20 05:38:55.477][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:98] #9:
[0x5563a39fa8c3]
conf-jira-envoy | [2020-11-20 05:38:55.478][73][critical][backtrace] [bazel-out/k8-opt/bin/source/server/_virtual_includes/backtrace_lib/server/backtrace.h:96] #10: start_thread
[0x7f9c2d4086db]
conf-jira-envoy exited with code 139
```

 **3ks** added bug triage labels on Nov 20, 2020

 **cpakulski** mentioned this issue on Nov 20, 2020

udp: properly handle truncated/dropped datagrams #14122

 Merged

mattklein123 commented on Nov 20, 2020

Member

Note this is a zero day that was under embargo. Fixes are going out now: [#14122](#)

 **mattklein123** closed this as completed in [#14122](#) on Nov 20, 2020

3ks commented on Nov 21, 2020

Contributor

Author

Incredible speed of restoration, Thanks for your work!

mattklein123 commented on Nov 21, 2020

Member

@3ks

| Incredible speed of restoration, Thanks for your work!

This issue was under embargo and you explicitly *did not follow* our security policy to report crashing issues to envoy-security@. *Do not do this again.*

3ks commented on Nov 22, 2020

Contributor

Author

| This issue was under embargo and you explicitly did not follow our security policy to report crashing issues to envoy-security@. Do not do this again.

@mattklein123 I'm sorry about that and I won't do it again.

 This was referenced on Nov 24, 2020

backport to 1.15: udp: properly handle truncated/dropped datagrams (#14122) #14166



 Merged

backport to 1.14: udp: properly handle truncated/dropped datagrams (#14122) #14192

 Merged

backport to 1.13: udp: properly handle truncated/dropped datagrams (#14122) #14198

 Merged

  asraa mentioned this issue on Feb 1, 2021

UDP proxy fuzzing #14889

 Closed

  ashxjain mentioned this issue on Aug 4, 2021

EDGECLLOUD-5230: Envoy crashing for UDP packet size larger than 1500 mobiledegex/edge-cloud#1443

 Merged

Assignees

No one assigned

Labels

bug triage

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 [udp: properly handle truncated/dropped datagrams](#)
cpakulski/envoy

2 participants

