



# CVE-2020-35471

Published on: 12/14/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:48 PM UTC

## CVE-2020-35471

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Envoy](#) from [Envoyproxy](#) contain the following vulnerability:

Envoy before 1.16.1 mishandles dropped and truncated datagrams, as demonstrated by a segmentation fault for a UDP packet size larger than 1500.

CVE-2020-35471 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>NONE</b>       | <b>PARTIAL</b>      |

## CVE References

| Description                                             | Tags                                                                                                                     | Link                                                                                                                                                      |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Comparing v1.16.0...v1.16.1 · envoyproxy/envoy · GitHub | <a href="#">Patch</a><br><a href="#">Third Party Advisory</a><br><a href="#">github.com</a><br><a href="#">text/html</a> | <a href="#">MISC</a><br><a href="https://github.com/envoyproxy/envoy/compare/v1.16.0...v1.16.1">github.com/envoyproxy/envoy/compare/v1.16.0...v1.16.1</a> |

udp: properly handle truncated/dropped datagrams by cpakulski · Pull Request #14122 · envoyproxy/envoy · GitHub

Patch

Third Party Advisory

github.com

text/html

MISC github.com/envoyproxy/envoy/pull/14122

crash when udp packet size large than 1500 · Issue #14113 · envoyproxy/envoy · GitHub

Exploit

Third Party Advisory

github.com

text/html

MISC github.com/envoyproxy/envoy/issues/14113

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

| Known Affected Configurations (CPE V2.3) |            |         |         |        |         |          |
|------------------------------------------|------------|---------|---------|--------|---------|----------|
| Type                                     | Vendor     | Product | Version | Update | Edition | Language |
| Application                              | Envoyproxy | Envoy   | All     | All    | All     | All      |
| Application                              | Envoyproxy | Envoy   | All     | All    | All     | All      |
| cpe:2.3:a:envoyproxy:envoy:*****:*       |            |         |         |        |         |          |
| cpe:2.3:a:envoyproxy:envoy:*****:*       |            |         |         |        |         |          |

No vendor comments have been submitted for this CVE

| Social Mentions                               |       |              |
|-----------------------------------------------|-------|--------------|
| Source                                        | Title | Posted (UTC) |
| <div>← Previous ID</div> <div>Next ID →</div> |       |              |