



CVE-2019-15226

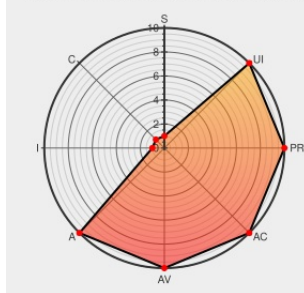
Published on: 10/09/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:44 PM UTC

CVE-2019-15226

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



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

Upon receiving each incoming request header data, Envoy will iterate over existing request headers to verify that the total size of the headers stays below a maximum limit. The implementation in versions 1.10.0 through 1.11.1 for HTTP/1.x traffic and all versions of Envoy for HTTP/2 traffic had $O(n^2)$ performance characteristics. A remote

attacker may craft a request that stays below the maximum request header size but consists of many thousands of small headers to consume CPU and result in a denial-of-service attack.

CVE-2019-15226 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
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **7.8 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Track byteSize of	CVE-2019-15226	MISC

Track byteSize of HeaderMap internally. · envoyproxy/envoy@afc39be · GitHub

PatchThird Party Advisorygithub.comtext/html

MISCgithub.com/envoyproxy/envoy/commit/afc39bea36fd436e54262f150c009e8d72dbf

CVE-2019-15226 · Issue #8520 · envoyproxy/envoy · GitHub

Third Party Advisorygithub.comtext/html

MISCgithub.com/envoyproxy/envoy/issues/8520

Commits · envoyproxy/envoy · GitHub

Third Party Advisoryweb.archive.orgtext/htmlInactive LinkNot Archived

MISCgithub.com/envoyproxy/envoy/commits/master

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.

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	1.0.0	All	All	All
Application	Envoyproxy	Envoy	1.1.0	All	All	All
Application	Envoyproxy	Envoy	1.10.0	All	All	All
Application	Envoyproxy	Envoy	1.11.0	All	All	All
Application	Envoyproxy	Envoy	1.11.1	All	All	All
Application	Envoyproxy	Envoy	1.11.2	All	All	All
Application	Envoyproxy	Envoy	1.2.0	All	All	All
Application	Envoyproxy	Envoy	1.3.0	All	All	All
Application	Envoyproxy	Envoy	1.4.0	All	All	All
Application	Envoyproxy	Envoy	1.5.0	All	All	All
Application	Envoyproxy	Envoy	1.6.0	All	All	All
Application	Envoyproxy	Envoy	1.7.0	All	All	All
Application	Envoyproxy	Envoy	1.7.1	All	All	All
Application	Envoyproxy	Envoy	1.8.0	All	All	All
Application	Envoyproxy	Envoy	1.9.0	All	All	All
Application	Envoyproxy	Envoy	1.9.1	All	All	All
Application	Envoyproxy	Envoy	1.0.0	All	All	All
Application	Envoyproxy	Envoy	1.1.0	All	All	All
Application	Envoyproxy	Envoy	1.10.0	All	All	All
Application	Envoyproxy	Envoy	1.11.0	All	All	All

Application	Envoyproxy	Envoy	1.11.1	All	All	All
Application	Envoyproxy	Envoy	1.11.2	All	All	All
Application	Envoyproxy	Envoy	1.2.0	All	All	All
Application	Envoyproxy	Envoy	1.3.0	All	All	All
Application	Envoyproxy	Envoy	1.4.0	All	All	All
Application	Envoyproxy	Envoy	1.5.0	All	All	All
Application	Envoyproxy	Envoy	1.6.0	All	All	All
Application	Envoyproxy	Envoy	1.7.0	All	All	All
Application	Envoyproxy	Envoy	1.7.1	All	All	All
Application	Envoyproxy	Envoy	1.8.0	All	All	All
Application	Envoyproxy	Envoy	1.9.0	All	All	All
Application	Envoyproxy	Envoy	1.9.1	All	All	All
cpe:2.3:a:envoyproxy:envoy:1.0.0:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.1.0:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.10.0:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.11.0:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.11.1:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.11.2:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.2.0:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.3.0:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.4.0:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.5.0:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.6.0:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.7.0:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.7.1:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.8.0:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.9.0:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.9.1:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.0.0:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.1.0:****:*:*:						
cpe:2.3:a:envoyproxy:envoy:1.10.0:****:*:*:						

cpe:2.3:a:envoyproxy:envoy:1.11.0:*****:
cpe:2.3:a:envoyproxy:envoy:1.11.1:*****:
cpe:2.3:a:envoyproxy:envoy:1.11.2:*****:
cpe:2.3:a:envoyproxy:envoy:1.2.0:*****:
cpe:2.3:a:envoyproxy:envoy:1.3.0:*****:
cpe:2.3:a:envoyproxy:envoy:1.4.0:*****:
cpe:2.3:a:envoyproxy:envoy:1.5.0:*****:
cpe:2.3:a:envoyproxy:envoy:1.6.0:*****:
cpe:2.3:a:envoyproxy:envoy:1.7.0:*****:
cpe:2.3:a:envoyproxy:envoy:1.7.1:*****:
cpe:2.3:a:envoyproxy:envoy:1.8.0:*****:
cpe:2.3:a:envoyproxy:envoy:1.9.0:*****:
cpe:2.3:a:envoyproxy:envoy:1.9.1:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)