



# CVE-2021-32715

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-32715
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-07-07 20:15:00 UTC
<b>Updated</b>	2021-07-22 12:49:00 UTC
<b>Description</b>	hyper is an HTTP library for rust. hyper's HTTP/1 server code had a flaw that incorrectly parses and accepts requests with c

## Risk And Classification

**Problem Types:** CWE-444

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Hyper</a>	<a href="#">Hyper</a>	All	All	All	All

## References

Reference	Source	Link
Lenient Parsing of Content-Length Header When Prefixed with Plus Sign · Advisory · hyperium/hyper · GitHub	CONFIRM	<a href="#">github.com</a>
Integer parsing should accept leading plus by arthurprs · Pull Request #28826 · rust-lang/rust · GitHub	MISC	<a href="#">github.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[182602](#) Debian Security Update for rust-hyper (CVE-2021-32715)

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)