



# CVE-2020-8910

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

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2020-8910                                                                                                              |
| <b>State</b>           | PUBLIC                                                                                                                     |
| <b>Assigner</b>        | security@google.com                                                                                                        |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2020-03-26 12:15:00 UTC                                                                                                    |
| <b>Updated</b>         | 2023-11-07 03:26:00 UTC                                                                                                    |
| <b>Description</b>     | A URL parsing issue in goog.uri of the Google Closure Library versions up to and including v20200224 allows an attacker to |

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product                         | Version | Update | Edition | Language |
|-------------|------------------------|---------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Google</a> | <a href="#">Closure Library</a> | All     | All    | All     | All      |
| Application | <a href="#">Google</a> | <a href="#">Closure Library</a> | All     | All    | All     | All      |

## References

| Reference                                                                              | Source  | Link                         | Tags                     |
|----------------------------------------------------------------------------------------|---------|------------------------------|--------------------------|
| Fix authority parsing in Closure URI parser. · google/closure-library@294fc00 · GitHub | CONFIRM | <a href="#">github.com</a>   | Patch, Third Party Advis |
| Release Closure Library v20200315 · google/closure-library · GitHub                    | CONFIRM | <a href="#">github.com</a>   | Third Party Advisory     |
| CVE Program record                                                                     | CVE.ORG | <a href="#">www.cve.org</a>  | canonical                |
| NVD vulnerability detail                                                               | NVD     | <a href="#">nvd.nist.gov</a> | canonical, analysis      |

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** David Schütz

**LEGACY:** François Lajeunesse-Robert

## Legacy QID Mappings

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)