



# CVE-2020-1896

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2020-1896   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve-assign@fb.com   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2021-02-02 07:15:00 UTC   |
| <b>Updated</b>         | 2021-03-26 19:17:00 UTC   |
| <b>Description</b>     | A stack overflow vulnerability in Facebook Hermes 'builtin apply' prior to commit 86543ac47e59c522976b5632b8bf9a2a458 |

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                   | Product                | Version | Update | Edition | Language |
|-------------|--------------------------|------------------------|---------|--------|---------|----------|
| Application | <a href="#">Facebook</a> | <a href="#">Hermes</a> | All     | All    | All     | All      |
| Application | <a href="#">Facebook</a> | <a href="#">Hermes</a> | All     | All    | All     | All      |

## References

| Reference   | Source  | Link                             |
|---|---------|----------------------------------|
| Added stack overflow check for hermes::vm:: hermesBuiltinApply · facebook/hermes@86543ac · GitHub | CONFIRM | <a href="#">github.com</a>       |
| Facebook  | CONFIRM | <a href="#">www.facebook.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.

There are currently no legacy QID mappings associated with this CVE.

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](#).

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