



CVE-2020-15234

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2020-15234 |
| State | PUBLIC |
| Assigner | security-advisories@github.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-10-02 21:15:00 UTC |
| Updated | 2021-11-18 16:52:00 UTC |
| Description | ORY Fosite is a security first OAuth2 & OpenID Connect framework for Go. In Fosite before version 0.34.1, the OAuth 2.0 C |

Risk And Classification

Problem Types: CWE-178

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|---------------------|------------------------|---------|--------|---------|----------|
| Application | Ory | Fosite | All | All | All | All |
| Application | Ory | Fosite | All | All | All | All |

References

| Reference | Source | Link | Tags |
|---|---------|------------------------------|-----------------------------|
| Redirect URL matching ignores character casing · Advisory · ory/fosite · GitHub | CONFIRM | github.com | Third Party Advisory |
| fix: make redirect URL checking more strict · ory/fosite@cdee51e · GitHub | MISC | github.com | Patch, Third Party Advisory |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[980060](#) Go (go) Security Update for github.com/ory/fosite (GHSA-grfp-q2mm-hfp6)

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](#).

CVE.report and Source URL Uptime Status status.cve.report