



# CVE-2020-26244

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

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2020-26244                                                                                                             |
| <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>       | 2020-12-02 20:15:00 UTC                                                                                                    |
| <b>Updated</b>         | 2020-12-08 02:37:00 UTC                                                                                                    |
| <b>Description</b>     | Python oic is a Python OpenID Connect implementation. In Python oic before version 1.2.1, there are several related cryptc |

## Risk And Classification

### Problem Types: CWE-347

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                                        | Product                               | Version | Update | Edition | Language |
|-------------|-----------------------------------------------|---------------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Python Openid Connect Project</a> | <a href="#">Python Openid Connect</a> | All     | All    | All     | All      |
| Application | <a href="#">Python Openid Connect Project</a> | <a href="#">Python Openid Connect</a> | All     | All    | All     | All      |

## References

| Reference                                                                                        | Source  | Link                         | Tags           |
|--------------------------------------------------------------------------------------------------|---------|------------------------------|----------------|
| Client vulnerabilites to replay attack and cipher downgrade · Advisory · OpenIDC/pyoidc · GitHub | CONFIRM | <a href="#">github.com</a>   | Third Party A  |
| Merge pull request from GHSA-4fjv-pmhg-3rfg · OpenIDC/pyoidc@62f8d75 · GitHub                    | MISC    | <a href="#">github.com</a>   | Patch, Third F |
| oic · PyPI                                                                                       | MISC    | <a href="#">pypi.org</a>     | Product, Venc  |
| Release Security vulnerability fix (CVE-2020-26244) · OpenIDC/pyoidc · GitHub                    | MISC    | <a href="#">github.com</a>   | Third Party A  |
| CVE Program record                                                                               | CVE.ORG | <a href="#">www.cve.org</a>  | canonical      |
| NVD vulnerability detail                                                                         | NVD     | <a href="#">nvd.nist.gov</a> | canonical, an  |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[983086](#) Python (pip) Security Update for oic (GHSA-4fjv-pmhg-3rfg)

© [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](#)