



# CVE-2019-16791

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

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2019-16791                                                                                                              |
| <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>       | 2020-01-22 02:15:00 UTC                                                                                                     |
| <b>Updated</b>         | 2020-10-23 18:18:00 UTC                                                                                                     |
| <b>Description</b>     | In postfix-mta-sts-resolver before 0.5.1, All users can receive incorrect response from daemon under rare conditions, rende |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                                           | Product                                  | Version | Update | Edition | Language |
|-------------|--------------------------------------------------|------------------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Postfix-mta-sts-resolver Project</a> | <a href="#">Postfix-mta-sts-resolver</a> | All     | All    | All     | All      |
| Application | <a href="#">Postfix-mta-sts-resolver Project</a> | <a href="#">Postfix-mta-sts-resolver</a> | All     | All    | All     | All      |

## References

| Reference                                                                      | Source  | Link                            | Tags                        |
|--------------------------------------------------------------------------------|---------|---------------------------------|-----------------------------|
| Incorrect query parsing · Advisory · Snawoot/postfix-mta-sts-resolver · GitHub | CONFIRM | <a href="#">github.com</a>      | Patch, Third Party Advisory |
| pmsr-0.2.9-parsing.patch · GitHub                                              | MISC    | <a href="#">gist.github.com</a> | Patch, 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         |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[983068](#) Python (pip) Security Update for postfix-mta-sts-resolver (GHSA-h92m-42h4-82f6)

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](https://cve.report/api)

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