



# CVE-2017-15093

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

## Summary

|                        |                                                                                                                                                                                                                                                                                                                                        |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2017-15093                                                                                                                                                                                                                                                                                                                         |
| <b>State</b>           | PUBLIC                                                                                                                                                                                                                                                                                                                                 |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                                                                                                                                                                                                                                    |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                                                                                                                                                                                                                           |
| <b>Published</b>       | 2018-01-23 15:29:00 UTC                                                                                                                                                                                                                                                                                                                |
| <b>Updated</b>         | 2019-10-09 23:24:00 UTC                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>     | When api-config-dir is set to a non-empty value, which is not the case by default, the API in PowerDNS Recursor 4.x up to 4.4.0-rc1 is vulnerable to a directory traversal attack. An attacker can use this vulnerability to read files from the local file system, including sensitive information like configuration files and logs. |

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

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

## References

| Reference                                                                                                     | Source  | Link                                                    |
|---------------------------------------------------------------------------------------------------------------|---------|---------------------------------------------------------|
| PowerDNS Security Advisory 2017-06: Configuration file injection in the API — PowerDNS Recursor documentation | CONFIRM | <a href="#">doc.powerdns.org/secadv/2017-06/</a>        |
| 101982                                                                                                        | BID     | <a href="#">www.securityfocus.com/bid/101982</a>        |
| CVE Program record                                                                                            | CVE.ORG | <a href="#">www.cve.org/CVE.expanded/CVE@2017-15093</a> |
| NVD vulnerability detail                                                                                      | NVD     | <a href="#">nvd.nist.gov/vuln/detail/CVE-2017-15093</a> |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[501110](#) Alpine Linux Security Update for pdns-recursor

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

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