



# CVE-2017-7557

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

## Summary

<b>CVE</b>	CVE-2017-7557
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-08-22 14:29:00 UTC
<b>Updated</b>	2019-10-09 23:29:00 UTC
<b>Description</b>	dnssdist version 1.1.0 is vulnerable to a flaw in authentication mechanism for REST API potentially allowing CSRF attack.

## Risk And Classification

**Problem Types:** CWE-352

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Powerdns</a>	<a href="#">Dnsdist</a>	1.1.0	All	All	All
Application	<a href="#">Powerdns</a>	<a href="#">Dnsdist</a>	1.1.0	All	All	All

## References

Reference	Source
<a href="#">PowerDNS Security Advisory 2017-02 for dnsdist: Alteration of ACLs via API authentication bypass — dnsdist documentation</a>	MISC
<a href="#">dnsdist CVE-2017-7557 Authentication Bypass Vulnerability</a>	BID
<a href="#">CVE Program record</a>	CVE.ORG
<a href="#">NVD vulnerability detail</a>	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[754154](#) SUSE Enterprise Linux Security Update for dnsdist (SUSE-SU-2023:2777-1)

[755904](#) SUSE Enterprise Linux Security Update for dnsdist (SUSE-SU-2023:2760-2)

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](#).

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