CVE-2016-7069

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-7069
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-11 13:29:00 UTC
Updated	2019-10-09 23:19:00 UTC
Description	An issue has been found in dnsdist before 1.2.0 in the way EDNS0 OPT records are handled when parsing responses from

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Powerdns	Dnsdist	All	All	x86	All

References

Reference	Sou
1483870 – (CVE-2016-7069) CVE-2016-7069 dnsdist: Crafted backend responses can cause a denial of service	CON
dnsdist CVE-2016-7069 Denial of Service Vulnerability	BID
PowerDNS Security Advisory 2017-01 for dnsdist: Crafted backend responses can cause a denial of service — dnsdist documentation	CON
CVE Program record	CVE
NVD vulnerability detail	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)

© 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 registred 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