



CVE-2018-5740

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

Summary

CVE	CVE-2018-5740
State	PUBLIC
Assigner	security-officer@isc.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-16 20:29:00 UTC
Updated	2022-04-12 18:34:00 UTC
Description	"deny-answer-aliases" is a little-used feature intended to help recursive server operators protect end users against DNS rek

Risk And Classification

Problem Types: CWE-617

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Hp	Hp-ux	-	All	All	All
Application	Isc	Bind	All	All	All	All
Application	Isc	Bind	All	All	All	All
Application	Netapp	Data Ontap Edge	-	All	All	All
Application	Netapp	Data Ontap Edge	-	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All

Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference	Source	Link
ISC BIND CVE-2018-5740 Remote Denial of Service Vulnerability	BID	www
BIND 'deny-answer-aliases' Bug Lets Remote Users Cause the Target 'named' Service to Crash - SecurityTracker	SECTRACK	www
BIND: Multiple vulnerabilities (GLSA 201903-13) — Gentoo security	GENTOO	sec
[security-announce] openSUSE-SU-2019:1533-1: important: Security update	SUSE	list
Security Advisories-CVE-2018-5740: A flaw in the "deny-answer-aliases" feature can cause an assertion failure in named	CONFIRM	kb.
CVE-2018-5740 ISC Bind Vulnerability in NetApp Products NetApp Product Security	CONFIRM	sec
Red Hat Customer Portal	REDHAT	acc
Red Hat Customer Portal	REDHAT	acc
[SECURITY] [DLA 2807-1] bind9 security update	MLIST	list
[SECURITY] [DLA 1485-1] bind9 security update	MLIST	list
USN-3769-1: Bind vulnerability Ubuntu security notices Ubuntu	UBUNTU	usi
HPE Support document - HPE Support Center	CONFIRM	sup
USN-3769-1: Bind vulnerability Ubuntu security notices Ubuntu	UBUNTU	

USN-3/69-2: Bind vulnerability Ubuntu security notices	UBUNTU	USN
[security-announce] openSUSE-SU-2019:1532-1: important: Security update	SUSE	list
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

Vendor Comments And Credit

Discovery Credit

LEGACY: ISC would like to thank Tony Finch of the University of Cambridge for reporting this issue.

Legacy QID Mappings

- [178863](#) Debian Security Update for bind9 (DLA 2807-1)
- [500051](#) Alpine Linux Security Update for bind
- [503732](#) Alpine Linux Security Update for bind
- [710200](#) Gentoo Linux BIND Multiple Vulnerabilities (GLSA 201903-13)

© [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](#).

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