CVE-2017-3145

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-3145
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	2023-06-21 18:19:00 UTC
Description	BIND was improperly sequencing cleanup operations on upstream recursion fetch contexts, leading in some cases to a use

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	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	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Isc	Bind	9.10.5	s1	All	All
Application	Isc	Bind	9.10.6	s1	All	All
Application	Isc	Bind	9.12.0	alpha1	All	All
Application	Isc	Bind	9.12.0	b1	All	All
Application	Isc	Bind	9.12.0	b2	All	All
Application	Isc	Bind	9.12.0	rc1	All	All
Application	Isc	Bind	9.9.11	s1	All	All
Application	Isc	Bind	9.9.3	s1	All	All
Application	Isc	Bind	9.10.5	s1	All	All
Application	Isc	Bind	9.10.6	s1	All	All
Application	Isc	Bind	9.12.0	alpha1	All	All

Application	Isc	Bind	9.12.0	b1	All	All
Application	Isc	Bind	9.12.0	b2	All	All
Application	Isc	Bind	9.12.0	rc1	All	All
Application	Isc	Bind	9.9.11	s1	All	All
Application	Isc	Bind	9.9.3	s1	All	All
Application	Isc	Bind	All	All	All	All
Application	Isc	Bind	All	All	All	All
Application	Isc	Bind	All	All	All	All
Application	Isc	Bind	All	All	All	All
Operating System	Juniper	Junos	12.1x46-d76	-	All	All
Operating System	Juniper	Junos	12.3x48-d70	-	All	All
Operating System	Juniper	Junos	15.1x49-d140	-	All	All
Operating System	Juniper	Junos	17.4r2	-	All	All
Operating System	Juniper	Junos	18.1r2	-	All	All
Operating System	Juniper	Junos	18.2r1	-	All	All
Hardware	Juniper	Srx100	-	All	All	All
Hardware	Juniper	Srx110	-	All	All	All
Hardware	Juniper	Srx1400	-	All	All	All
Hardware	Juniper	Srx1500	-	All	All	All
Hardware	Juniper	Srx210	-	All	All	All
Hardware	Juniper	Srx220	-	All	All	All
Hardware	Juniper	Srx240	-	All	All	All
Hardware	Juniper	Srx240h2	-	All	All	All
Hardware	Juniper	Srx240m	-	All	All	All
Hardware	Juniper	Srx300	-	All	All	All
Hardware	Juniper	Srx320	-	All	All	All
Hardware	Juniper	Srx340	-	All	All	All
Hardware	Juniper	Srx3400	-	All	All	All
Hardware	Juniper	Srx345	-	All	All	All
Hardware	Juniper	Srx3600	-	All	All	All
Hardware	Juniper	Srx380	-	All	All	All
Hardware	Juniper	Srx4000	-	All	All	All
Hardware	Juniper	Srx4100	-	All	All	All
Hardware	Juniper	Srx4200	-	All	All	All
Hardware	Juniper	Srx4600	-	All	All	All

Hardware	Juniper	Srx5000	-	All	All	All
Hardware	Juniper	Srx5400	-	All	All	All
Hardware	Juniper	Srx550	-	All	All	All
Hardware	Juniper	Srx550m	-	All	All	All
Hardware	Juniper	Srx550 Hm	-	All	All	All
Hardware	Juniper	Srx5600	-	All	All	All
Hardware	Juniper	Srx5800	-	All	All	All
Hardware	Juniper	Srx650	-	All	All	All
Application	Netapp	Data Ontap Edge	-	All	All	All
Application	Netapp	Data Ontap Edge	-	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	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	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	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	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 Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	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
CEC Juniper Community	MISC
Red Hat Customer Portal	REDHAT
CVE-2017-3145 ISC BIND Vulnerability in NetApp Products | NetApp Product Security	CONFIRM
Debian -- Security Information -- DSA-4089-1 bind9	DEBIAN
[SECURITY] [DLA 1255-1] bind9 security update	MLIST
ISC BIND CVE-2017-3145 Remote Denial of Service Vulnerability	BID
BIND Recursion Processing Error in 'netaddr.c' Lets Remote Users Cause the Target 'named' Service to Crash - SecurityTracker	SECTRAC
Red Hat Customer Portal	REDHAT
CVE-2017-3145: Improper fetch cleanup sequencing in the resolver can cause named to crash - Security Advisories	CONFIRM
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500049 Alpine Linux Security Update for bind

503730 Alpine Linux Security Update for bind