CVE-2016-6170

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-6170
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-07-06 14:59:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	ISC BIND through 9.9.9-P1, 9.10.x through 9.10.4-P1, and 9.11.x through 9.11.0b1 allows primary DNS servers to cause a

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Problem Types: CWE-20 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	4		AV:N/AC:L/Au:S/C:N/I:N/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:S/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Isc	Bind	9.10.4	-	All	All
Application	Isc	Bind	9.10.4	p1	All	All
Application	Isc	Bind	9.11.0	a1	All	All
Application	Isc	Bind	9.11.0	a2	All	All
Application	Isc	Bind	9.11.0	a3	All	All
Application	Isc	Bind	9.11.0	b1	All	All
Application	Isc	Bind	9.9.9	-	All	All
Application	Isc	Bind	9.9.9	beta1	All	All
Application	Isc	Bind	9.9.9	beta2	All	All
Application	Isc	Bind	9.9.9	p1	All	All
Application	Isc	Bind	All	All	All	All
Application	Isc	Bind	All	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
1353563 – (CVE-2016-6170) CVE-2016-6170 bind: Improper restriction of zone size limit
[dns-operations] DNS activities in Japan
ISC BIND CVE-2016-6170 Remote Denial of Service Vulnerability
[dns-operations] DNS activities in Japan
oss-security - Malicious primary DNS servers can crash secondaries
BIND: Multiple vulnerabilities (GLSA 201610-07) — Gentoo Security
xfer-limit/README.md at master · sischkg/xfer-limit · GitHub
BIND AXFR/IXFR Response Processing Flaw Lets Remote DNS Servers to Cause the Target DNS Service to Crash - SecurityTracker
[dns-operations] DNS activities in Japan
Operational Notification: A party that is allowed control over zone data can overwhelm a server by transferring huge quantities of data. - Opera
Operational Notification: A party that is allowed control over zone data can overwhelm a server by transferring huge quantities of data. | Interne
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.