CVE-2010-3615

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

Summary

CVE	CVE-2010-3615
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-12-06 13:44:54 UTC
Updated	2026-04-29 01:13:23 UTC
Description	named in ISC BIND 9.7.2-P2 does not check all intended locations for allow-query ACLs, which might allow remote attacker

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Isc	Bind	9.7.2	p2	All	All

Vendor Declared Affected Products

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

References

Reference	Source
The Slackware Linux Project: Slackware Security Advisories	af854a3a-2127-422b-91ae-364da2661108
US-CERT Vulnerability Note VU#510208	af854a3a-2127-422b-91ae-364da2661108
Guidance regarding Dec 1st 2010 Security Advisories | Internet Systems Consortium	af854a3a-2127-422b-91ae-364da2661108
BIND: allow-query processed incorrectly | Internet Systems Consortium	af854a3a-2127-422b-91ae-364da2661108
[SECURITY] Fedora 14 Update: bind-9.7.2-4.P3.fc14	af854a3a-2127-422b-91ae-364da2661108
osvdb.org/69568	af854a3a-2127-422b-91ae-364da2661108
SecurityTracker: BIND Bugs Let Remote Users Bypass Access Controls and Deny Service	af854a3a-2127-422b-91ae-364da2661108
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108
Slackware update for bind - Advisories - Community	af854a3a-2127-422b-91ae-364da2661108
Security Advisory SA42458 - BIND "allow-query" ACL Bypass Vulnerability - Secunia	af854a3a-2127-422b-91ae-364da2661108
ISC BIND 'allow-query' Zone ACL Security Bypass Vulnerability	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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