CVE-2010-0213

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

Summary

CVE	CVE-2010-0213
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-07-28 12:48:00 UTC
Updated	2016-04-04 15:50:00 UTC
Description	BIND 9.7.1 and 9.7.1-P1, when a recursive validating server has a trust anchor that is configured statically or via DNSSEC

Risk And Classification

Problem Types: CWE-19

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Isc	Bind	9.7.1	All	All	All
Application	Isc	Bind	9.7.1	p1	All	All
Application	Isc	Bind	9.7.1	All	All	All
Application	Isc	Bind	9.7.1	p1	All	All

References

Reference	Source	Link
CERT Vulnerability Notes Database	CERT-VN	www.kb.cert.org
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
[SECURITY] Fedora 13 Update: bind-9.7.1-2.P2.fc13	FEDORA	lists.fedoraproject.o
BIND "RRSIG" Requests Endless Loop Denial of Service - Advisories - Community	SECUNIA	secunia.com
SecurityTracker.com Archives - BIND 'RRSIG' Query Processing Error Lets Remote Users Deny Service	SECTRACK	www.securitytracke
RRSIG query handling bug in BIND 9.7.1 | Internet Systems Consortium	CONFIRM	www.isc.org
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:020	SUSE	lists.opensuse.org
ISC BIND 9 'RRSIG' Record Type Remote Denial of Service Vulnerability	BID	www.securityfocus.
Fedora update for bind - Advisories - Community	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org

NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**