



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.org
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.securitytracker.com
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.com
Fedora update for bind - Advisories - Community	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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