



CVE-2007-0494

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2007-0494
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-01-25 20:28:00 UTC
Updated	2017-10-11 01:31:00 UTC
Description	ISC BIND 9.0.x, 9.1.x, 9.2.0 up to 9.2.7, 9.3.0 up to 9.3.3, 9.4.0a1 up to 9.4.0a6, 9.4.0b1 up to 9.4.0b4, 9.4.0rc1, and 9.5.0a

Risk And Classification

Problem Types: CWE-19

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Isc	Bind	9.0	All	All	All
Application	Isc	Bind	9.0.0	rc1	All	All
Application	Isc	Bind	9.0.0	rc2	All	All
Application	Isc	Bind	9.0.0	rc3	All	All
Application	Isc	Bind	9.0.0	rc4	All	All
Application	Isc	Bind	9.0.0	rc5	All	All
Application	Isc	Bind	9.0.0	rc6	All	All
Application	Isc	Bind	9.0.1	All	All	All
Application	Isc	Bind	9.0.1	rc1	All	All
Application	Isc	Bind	9.0.1	rc2	All	All
Application	Isc	Bind	9.1	All	All	All
Application	Isc	Bind	9.1.0	rc1	All	All
Application	Isc	Bind	9.1.1	All	All	All
Application	Isc	Bind	9.1.1	rc1	All	All
Application	Isc	Bind	9.1.1	rc2	All	All
Application	Isc	Bind	9.1.1	rc3	All	All
Application	Isc	Bind	9.1.1	rc4	All	All

Application	lsc	Bind	9.1.1	rc5	All	All
Application	lsc	Bind	9.1.1	rc6	All	All
Application	lsc	Bind	9.1.1	rc7	All	All
Application	lsc	Bind	9.1.2	All	All	All
Application	lsc	Bind	9.1.2	rc1	All	All
Application	lsc	Bind	9.1.3	All	All	All
Application	lsc	Bind	9.1.3	rc1	All	All
Application	lsc	Bind	9.1.3	rc2	All	All
Application	lsc	Bind	9.1.3	rc3	All	All
Application	lsc	Bind	9.2	All	All	All
Application	lsc	Bind	9.2.0	All	All	All
Application	lsc	Bind	9.2.0	a1	All	All
Application	lsc	Bind	9.2.0	a2	All	All
Application	lsc	Bind	9.2.0	a3	All	All
Application	lsc	Bind	9.2.0	b1	All	All
Application	lsc	Bind	9.2.0	b2	All	All
Application	lsc	Bind	9.2.0	rc1	All	All
Application	lsc	Bind	9.2.0	rc10	All	All
Application	lsc	Bind	9.2.0	rc2	All	All
Application	lsc	Bind	9.2.0	rc3	All	All
Application	lsc	Bind	9.2.0	rc4	All	All
Application	lsc	Bind	9.2.0	rc5	All	All
Application	lsc	Bind	9.2.0	rc6	All	All
Application	lsc	Bind	9.2.0	rc7	All	All
Application	lsc	Bind	9.2.0	rc8	All	All
Application	lsc	Bind	9.2.0	rc9	All	All
Application	lsc	Bind	9.2.1	All	All	All
Application	lsc	Bind	9.2.1	rc1	All	All
Application	lsc	Bind	9.2.1	rc2	All	All
Application	lsc	Bind	9.2.2	All	All	All
Application	lsc	Bind	9.2.2	p2	All	All
Application	lsc	Bind	9.2.2	p3	All	All
Application	lsc	Bind	9.2.2	rc1	All	All
Application	lsc	Bind	9.2.3	All	All	All
Application	lsc	Bind	9.2.3	rc1	All	All

Application	lsc	Bind	9.2.3	rc2	All	All
Application	lsc	Bind	9.2.3	rc3	All	All
Application	lsc	Bind	9.2.3	rc4	All	All
Application	lsc	Bind	9.2.4	All	All	All
Application	lsc	Bind	9.2.4	rc2	All	All
Application	lsc	Bind	9.2.4	rc3	All	All
Application	lsc	Bind	9.2.4	rc4	All	All
Application	lsc	Bind	9.2.4	rc5	All	All
Application	lsc	Bind	9.2.4	rc6	All	All
Application	lsc	Bind	9.2.4	rc7	All	All
Application	lsc	Bind	9.2.4	rc8	All	All
Application	lsc	Bind	9.2.5	All	All	All
Application	lsc	Bind	9.2.5	b2	All	All
Application	lsc	Bind	9.2.5	rc1	All	All
Application	lsc	Bind	9.2.6	All	All	All
Application	lsc	Bind	9.2.6	rc1	All	All
Application	lsc	Bind	9.3	All	All	All
Application	lsc	Bind	9.3.0	All	All	All
Application	lsc	Bind	9.3.0	b2	All	All
Application	lsc	Bind	9.3.0	b3	All	All
Application	lsc	Bind	9.3.0	b4	All	All
Application	lsc	Bind	9.3.0	rc1	All	All
Application	lsc	Bind	9.3.0	rc2	All	All
Application	lsc	Bind	9.3.0	rc3	All	All
Application	lsc	Bind	9.3.0	rc4	All	All
Application	lsc	Bind	9.3.1	All	All	All
Application	lsc	Bind	9.3.1	b2	All	All
Application	lsc	Bind	9.3.1	rc1	All	All
Application	lsc	Bind	9.3.2	All	All	All
Application	lsc	Bind	9.3.2	rc1	All	All
Application	lsc	Bind	9.4.0	a1	All	All
Application	lsc	Bind	9.4.0	a2	All	All
Application	lsc	Bind	9.4.0	a3	All	All
Application	lsc	Bind	9.4.0	a4	All	All
Application	lsc	Bind	9.4.0	a5	All	All
Application	lsc	Bind	9.4.0	b1	All	All

Application	lsc	Bind	9.4.0	b1	All	All
Application	lsc	Bind	9.4.0	b2	All	All
Application	lsc	Bind	9.4.0	b3	All	All
Application	lsc	Bind	9.4.0	rc1	All	All
Application	lsc	Bind	9.5.0	a1	All	All
Application	lsc	Bind	9.0	All	All	All
Application	lsc	Bind	9.0.0	rc1	All	All
Application	lsc	Bind	9.0.0	rc2	All	All
Application	lsc	Bind	9.0.0	rc3	All	All
Application	lsc	Bind	9.0.0	rc4	All	All
Application	lsc	Bind	9.0.0	rc5	All	All
Application	lsc	Bind	9.0.0	rc6	All	All
Application	lsc	Bind	9.0.1	All	All	All
Application	lsc	Bind	9.0.1	rc1	All	All
Application	lsc	Bind	9.0.1	rc2	All	All
Application	lsc	Bind	9.1	All	All	All
Application	lsc	Bind	9.1.0	rc1	All	All
Application	lsc	Bind	9.1.1	All	All	All
Application	lsc	Bind	9.1.1	rc1	All	All
Application	lsc	Bind	9.1.1	rc2	All	All
Application	lsc	Bind	9.1.1	rc3	All	All
Application	lsc	Bind	9.1.1	rc4	All	All
Application	lsc	Bind	9.1.1	rc5	All	All
Application	lsc	Bind	9.1.1	rc6	All	All
Application	lsc	Bind	9.1.1	rc7	All	All
Application	lsc	Bind	9.1.2	All	All	All
Application	lsc	Bind	9.1.2	rc1	All	All
Application	lsc	Bind	9.1.3	All	All	All
Application	lsc	Bind	9.1.3	rc1	All	All
Application	lsc	Bind	9.1.3	rc2	All	All
Application	lsc	Bind	9.1.3	rc3	All	All
Application	lsc	Bind	9.2	All	All	All
Application	lsc	Bind	9.2.0	All	All	All
Application	lsc	Bind	9.2.0	a1	All	All
Application	lsc	Bind	9.2.0	a2	All	All
Application	lsc	Bind	9.2.0	a3	All	All

Application	lsc	Bind	9.2.0	b1	All	All
Application	lsc	Bind	9.2.0	b2	All	All
Application	lsc	Bind	9.2.0	rc1	All	All
Application	lsc	Bind	9.2.0	rc10	All	All
Application	lsc	Bind	9.2.0	rc2	All	All
Application	lsc	Bind	9.2.0	rc3	All	All
Application	lsc	Bind	9.2.0	rc4	All	All
Application	lsc	Bind	9.2.0	rc5	All	All
Application	lsc	Bind	9.2.0	rc6	All	All
Application	lsc	Bind	9.2.0	rc7	All	All
Application	lsc	Bind	9.2.0	rc8	All	All
Application	lsc	Bind	9.2.0	rc9	All	All
Application	lsc	Bind	9.2.1	All	All	All
Application	lsc	Bind	9.2.1	rc1	All	All
Application	lsc	Bind	9.2.1	rc2	All	All
Application	lsc	Bind	9.2.2	All	All	All
Application	lsc	Bind	9.2.2	p2	All	All
Application	lsc	Bind	9.2.2	p3	All	All
Application	lsc	Bind	9.2.2	rc1	All	All
Application	lsc	Bind	9.2.3	All	All	All
Application	lsc	Bind	9.2.3	rc1	All	All
Application	lsc	Bind	9.2.3	rc2	All	All
Application	lsc	Bind	9.2.3	rc3	All	All
Application	lsc	Bind	9.2.3	rc4	All	All
Application	lsc	Bind	9.2.4	All	All	All
Application	lsc	Bind	9.2.4	rc2	All	All
Application	lsc	Bind	9.2.4	rc3	All	All
Application	lsc	Bind	9.2.4	rc4	All	All
Application	lsc	Bind	9.2.4	rc5	All	All
Application	lsc	Bind	9.2.4	rc6	All	All
Application	lsc	Bind	9.2.4	rc7	All	All
Application	lsc	Bind	9.2.4	rc8	All	All
Application	lsc	Bind	9.2.5	All	All	All
Application	lsc	Bind	9.2.5	b2	All	All
Application	lsc	Bind	9.2.5	rc1	All	All

Application	lsc	Bind	9.2.6	All	All	All
Application	lsc	Bind	9.2.6	rc1	All	All
Application	lsc	Bind	9.3	All	All	All
Application	lsc	Bind	9.3.0	All	All	All
Application	lsc	Bind	9.3.0	b2	All	All
Application	lsc	Bind	9.3.0	b3	All	All
Application	lsc	Bind	9.3.0	b4	All	All
Application	lsc	Bind	9.3.0	rc1	All	All
Application	lsc	Bind	9.3.0	rc2	All	All
Application	lsc	Bind	9.3.0	rc3	All	All
Application	lsc	Bind	9.3.0	rc4	All	All
Application	lsc	Bind	9.3.1	All	All	All
Application	lsc	Bind	9.3.1	b2	All	All
Application	lsc	Bind	9.3.1	rc1	All	All
Application	lsc	Bind	9.3.2	All	All	All
Application	lsc	Bind	9.3.2	rc1	All	All
Application	lsc	Bind	9.4.0	a1	All	All
Application	lsc	Bind	9.4.0	a2	All	All
Application	lsc	Bind	9.4.0	a3	All	All
Application	lsc	Bind	9.4.0	a4	All	All
Application	lsc	Bind	9.4.0	a5	All	All
Application	lsc	Bind	9.4.0	b1	All	All
Application	lsc	Bind	9.4.0	b2	All	All
Application	lsc	Bind	9.4.0	b3	All	All
Application	lsc	Bind	9.4.0	rc1	All	All
Application	lsc	Bind	9.5.0	a1	All	All

References

Reference

2007-0005

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

rhn.redhat.com | Red Hat Support

FreeBSD update for bind - Advisories - Secunia

SGI Advanced Linux Environment 3 Multiple Updates - Advisories - Secunia

Ubuntu update for bind - Advisories - Secunia

'Internet Systems Consortium Security Advisory.' - MARC

#200061: Security Vulnerability in Solaris 10 BIND DNSSEC May Cause a Denial of Service
Sun Solaris 10 BIND DNSSEC Denial of Service - Advisories - Secunia
USN-418-1: Bind vulnerabilities Ubuntu
issues.rpath.com/browse/RPL-989
HP-UX update for Bind - Advisories - Secunia
ISC BIND Denial of Service Vulnerabilities - Advisories - Secunia
FreeBSD-SA-07:02
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Trustix update for bind and ed - Advisories - Secunia
SecurityTracker.com Archives - BIND DNSSEC Validation Bug Lets Remote Users Deny Service
Debian -- Security Information -- DSA-1254-1 bind9
[Full-Disclosure] Mailing List Charter
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
IBM notice: The page you requested cannot be displayed
HP Tru64 UNIX Multiple SSL and BIND Vulnerabilities - Advisories - Secunia
Gentoo Linux Documentation -- BIND: Denial of Service
rhn.redhat.com Red Hat Support
Document Display HPE Support Center
IBM notice: The page you requested cannot be displayed
IBM notice: The page you requested cannot be displayed
Advisories Mandriva
rPath update for bind and bind-utils - Advisories - Secunia
VMware ESX Server Multiple Security Updates - Advisories - Secunia
20070201-01-P
Fedora update for bind - Advisories - Secunia
SUSE update for bind - Advisories - Secunia
Gentoo update for vmware - Advisories - Secunia
SSRT061273
NetBSD-SA2007-003
ASA-2007-125 (RHSA-2007-0044)
ISC BIND Remote DNSSEC Validation Denial of Service Vulnerability
The Slackware Linux Project: Slackware Security Advisories
Fedora update for bind - Advisories - Secunia

IBM X-Force Exchange
Debian update for bind9 - Advisories - Secunia
APPLE-SA-2007-05-24 Security Update 2007-005
ISC has a new website Internet Systems Consortium
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
[SECURITY] Fedora Core 6 Update: bind-9.3.4-1.fc6 FedoraNEWS.ORG
[SECURITY] Fedora Core 5 Update: bind-9.3.4-1.fc5 FedoraNEWS.ORG
ISC has a new website Internet Systems Consortium
Webmail - OVH
Gentoo update for bind - Advisories - Secunia
Avaya Products bind Denial of Service - Advisories - Secunia
Red Hat update for bind - Advisories - Secunia
OpenPKG Corporation: Security: Security Advisories
HP Insight Management Agents SSL Vulnerabilities - Advisories - Secunia
Apple Mac OS X Security Update for Multiple Vulnerabilities - Advisories - Secunia
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: bind remote denial of service (SUSE-SA:2007:014)
IBM AIX BIND Denial of Service Vulnerability - Advisories - Secunia
Repository / Oval Repository
SSRT071304
ISC has a new website Internet Systems Consortium
Mandriva update for bind - Advisories - Secunia
IBM notice: The page you requested cannot be displayed
About Security Update 2007-005
Slackware update for bind - Advisories - Secunia
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.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). 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