



CVE-2009-0265

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

Summary

CVE	CVE-2009-0265
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-01-26 15:30:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	Internet Systems Consortium (ISC) BIND 9.6.0 and earlier does not properly check the return value from the OpenSSL EVF

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	lsc	Bind	4	All	All	All
Application	lsc	Bind	4.9	All	All	All
Application	lsc	Bind	4.9.10	All	All	All
Application	lsc	Bind	4.9.2	All	All	All
Application	lsc	Bind	4.9.3	All	All	All
Application	lsc	Bind	4.9.4	All	All	All
Application	lsc	Bind	4.9.5	All	All	All
Application	lsc	Bind	4.9.5	p1	All	All
Application	lsc	Bind	4.9.6	All	All	All
Application	lsc	Bind	4.9.7	All	All	All
Application	lsc	Bind	4.9.8	All	All	All
Application	lsc	Bind	4.9.9	All	All	All
Application	lsc	Bind	8	All	All	All
Application	lsc	Bind	8.1	All	All	All
Application	lsc	Bind	8.1.1	All	All	All
Application	lsc	Bind	8.1.2	All	All	All
Application	lsc	Bind	8.2	All	All	All

Application	lsc	Bind	8.2	p1	All	All
Application	lsc	Bind	8.2.1	All	All	All
Application	lsc	Bind	8.2.2	All	All	All
Application	lsc	Bind	8.2.2	p1	All	All
Application	lsc	Bind	8.2.2	p2	All	All
Application	lsc	Bind	8.2.2	p3	All	All
Application	lsc	Bind	8.2.2	p4	All	All
Application	lsc	Bind	8.2.2	p5	All	All
Application	lsc	Bind	8.2.2	p6	All	All
Application	lsc	Bind	8.2.2	p7	All	All
Application	lsc	Bind	8.2.3	All	All	All
Application	lsc	Bind	8.2.4	All	All	All
Application	lsc	Bind	8.2.5	All	All	All
Application	lsc	Bind	8.2.6	All	All	All
Application	lsc	Bind	8.2.7	All	All	All
Application	lsc	Bind	8.3.0	All	All	All
Application	lsc	Bind	8.3.1	All	All	All
Application	lsc	Bind	8.3.2	All	All	All
Application	lsc	Bind	8.3.3	All	All	All
Application	lsc	Bind	8.3.4	All	All	All
Application	lsc	Bind	8.3.5	All	All	All
Application	lsc	Bind	8.3.6	All	All	All
Application	lsc	Bind	8.4	All	All	All
Application	lsc	Bind	8.4.1	All	All	All
Application	lsc	Bind	8.4.4	All	All	All
Application	lsc	Bind	8.4.5	All	All	All
Application	lsc	Bind	8.4.7	All	All	All
Application	lsc	Bind	9.0	All	All	All
Application	lsc	Bind	9.0.1	All	All	All
Application	lsc	Bind	9.1	All	All	All
Application	lsc	Bind	9.1.1	All	All	All
Application	lsc	Bind	9.1.2	All	All	All
Application	lsc	Bind	9.1.3	All	All	All
Application	lsc	Bind	9.2	All	All	All
Application	lsc	Bind	9.2.0	All	All	All

Application	lsc	Bind	9.2.1	All	All	All
Application	lsc	Bind	9.2.2	All	All	All
Application	lsc	Bind	9.2.2	p3	All	All
Application	lsc	Bind	9.2.3	All	All	All
Application	lsc	Bind	9.2.4	All	All	All
Application	lsc	Bind	9.2.5	All	All	All
Application	lsc	Bind	9.2.6	All	All	All
Application	lsc	Bind	9.2.7	All	All	All
Application	lsc	Bind	9.2.9	All	All	All
Application	lsc	Bind	9.3	All	All	All
Application	lsc	Bind	9.3.0	All	All	All
Application	lsc	Bind	9.3.1	All	All	All
Application	lsc	Bind	9.3.2	All	All	All
Application	lsc	Bind	9.3.3	All	All	All
Application	lsc	Bind	9.3.5-p2-w1	windows	All	All
Application	lsc	Bind	9.4	All	All	All
Application	lsc	Bind	9.4.0	All	All	All
Application	lsc	Bind	9.4.0	rc1	All	All
Application	lsc	Bind	9.4.1	All	All	All
Application	lsc	Bind	9.4.2	All	All	All
Application	lsc	Bind	9.4.3	All	All	All
Application	lsc	Bind	9.4.3	rc1	All	All
Application	lsc	Bind	9.5.0	All	All	All
Application	lsc	Bind	9.5.0	rc1	All	All
Application	lsc	Bind	9.5.1	All	All	All
Application	lsc	Bind	9.5.1	rc1	All	All
Application	lsc	Bind	9.5.1	rc2	All	All
Application	lsc	Bind	9.6.0	All	All	All
Application	lsc	Bind	9.6.0	p1	All	All
Application	lsc	Bind	9.6.0	rc1	All	All
Application	lsc	Bind	9.6.0	rc2	All	All
Application	lsc	Bind	4	All	All	All
Application	lsc	Bind	4.9	All	All	All
Application	lsc	Bind	4.9.10	All	All	All
Application	lsc	Bind	4.9.2	All	All	All
Application	lsc	Bind	4.9.2	All	All	All

Application	lsc	Bind	4.9.3	All	All	All
Application	lsc	Bind	4.9.4	All	All	All
Application	lsc	Bind	4.9.5	All	All	All
Application	lsc	Bind	4.9.5	p1	All	All
Application	lsc	Bind	4.9.6	All	All	All
Application	lsc	Bind	4.9.7	All	All	All
Application	lsc	Bind	4.9.8	All	All	All
Application	lsc	Bind	4.9.9	All	All	All
Application	lsc	Bind	8	All	All	All
Application	lsc	Bind	8.1	All	All	All
Application	lsc	Bind	8.1.1	All	All	All
Application	lsc	Bind	8.1.2	All	All	All
Application	lsc	Bind	8.2	All	All	All
Application	lsc	Bind	8.2	p1	All	All
Application	lsc	Bind	8.2.1	All	All	All
Application	lsc	Bind	8.2.2	All	All	All
Application	lsc	Bind	8.2.2	p1	All	All
Application	lsc	Bind	8.2.2	p2	All	All
Application	lsc	Bind	8.2.2	p3	All	All
Application	lsc	Bind	8.2.2	p4	All	All
Application	lsc	Bind	8.2.2	p5	All	All
Application	lsc	Bind	8.2.2	p6	All	All
Application	lsc	Bind	8.2.2	p7	All	All
Application	lsc	Bind	8.2.3	All	All	All
Application	lsc	Bind	8.2.4	All	All	All
Application	lsc	Bind	8.2.5	All	All	All
Application	lsc	Bind	8.2.6	All	All	All
Application	lsc	Bind	8.2.7	All	All	All
Application	lsc	Bind	8.3.0	All	All	All
Application	lsc	Bind	8.3.1	All	All	All
Application	lsc	Bind	8.3.2	All	All	All
Application	lsc	Bind	8.3.3	All	All	All
Application	lsc	Bind	8.3.4	All	All	All
Application	lsc	Bind	8.3.5	All	All	All
Application	lsc	Bind	8.3.6	All	All	All
Application	lsc	Bind	8.4	All	All	All

Application	lsc	Bind	8.4.1	All	All	All
Application	lsc	Bind	8.4.4	All	All	All
Application	lsc	Bind	8.4.5	All	All	All
Application	lsc	Bind	8.4.7	All	All	All
Application	lsc	Bind	9.0	All	All	All
Application	lsc	Bind	9.0.1	All	All	All
Application	lsc	Bind	9.1	All	All	All
Application	lsc	Bind	9.1.1	All	All	All
Application	lsc	Bind	9.1.2	All	All	All
Application	lsc	Bind	9.1.3	All	All	All
Application	lsc	Bind	9.2	All	All	All
Application	lsc	Bind	9.2.0	All	All	All
Application	lsc	Bind	9.2.1	All	All	All
Application	lsc	Bind	9.2.2	All	All	All
Application	lsc	Bind	9.2.2	p3	All	All
Application	lsc	Bind	9.2.3	All	All	All
Application	lsc	Bind	9.2.4	All	All	All
Application	lsc	Bind	9.2.5	All	All	All
Application	lsc	Bind	9.2.6	All	All	All
Application	lsc	Bind	9.2.7	All	All	All
Application	lsc	Bind	9.2.9	All	All	All
Application	lsc	Bind	9.3	All	All	All
Application	lsc	Bind	9.3.0	All	All	All
Application	lsc	Bind	9.3.1	All	All	All
Application	lsc	Bind	9.3.2	All	All	All
Application	lsc	Bind	9.3.3	All	All	All
Application	lsc	Bind	9.3.5-p2-w1	windows	All	All
Application	lsc	Bind	9.4	All	All	All
Application	lsc	Bind	9.4.0	All	All	All
Application	lsc	Bind	9.4.0	rc1	All	All
Application	lsc	Bind	9.4.1	All	All	All
Application	lsc	Bind	9.4.2	All	All	All
Application	lsc	Bind	9.4.3	All	All	All
Application	lsc	Bind	9.4.3	rc1	All	All
Application	lsc	Bind	9.5.0	All	All	All

Application	lsc	Bind	9.5.0	rc1	All	All
Application	lsc	Bind	9.5.1	All	All	All
Application	lsc	Bind	9.5.1	rc1	All	All
Application	lsc	Bind	9.5.1	rc2	All	All
Application	lsc	Bind	9.6.0	All	All	All
Application	lsc	Bind	9.6.0	p1	All	All
Application	lsc	Bind	9.6.0	rc1	All	All
Application	lsc	Bind	9.6.0	rc2	All	All
Application	lsc	Bind	All	All	All	All

References

Reference	Source	Link
www.mandriva.com	MANDRIVA	www.mandriva.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Oops! - ISC	CONFIRM	www.isc.org
Slackware update for bind - Secunia.com	SECUNIA	secunia.com
BIND Security Advisory (CVE-2009-0025; Severity: Low) - comp.protocols.dns.bind Google Groups	MISC	groups.google.com
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE	slackware.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-01-26	Joshua Bressers	Not vulnerable. This issue did not affect the versions of BIND as shipped with Red Hat Ente

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

© [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](#) 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](#)