



CVE-2013-6230

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

Summary

CVE	CVE-2013-6230
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-11-08 04:47:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	The Winsock WSALocctl API in Microsoft Windows Server 2008, as used in ISC BIND 9.6-ESV before 9.6-ESV-R10-P1, 9.8

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Isc	Bind	9.6	All	All	All
Application	Isc	Bind	9.6	r5_p1	All	All
Application	Isc	Bind	9.6	r6_b1	All	All
Application	Isc	Bind	9.6	r6_rc1	All	All
Application	Isc	Bind	9.6	r6_rc2	All	All
Application	Isc	Bind	9.6	r7_p1	All	All
Application	Isc	Bind	9.6	r7_p2	All	All
Application	Isc	Bind	9.6	r9_p1	All	All
Application	Isc	Bind	9.8.0	All	All	All
Application	Isc	Bind	9.8.0	a1	All	All
Application	Isc	Bind	9.8.0	b1	All	All
Application	Isc	Bind	9.8.0	p1	All	All
Application	Isc	Bind	9.8.0	p2	All	All
Application	Isc	Bind	9.8.0	p4	All	All
Application	Isc	Bind	9.8.0	rc1	All	All
Application	Isc	Bind	9.8.1	All	All	All
Application	Isc	Bind	9.8.1	b1	All	All

Application	lsc	Bind	9.8.1	b2	All	All
Application	lsc	Bind	9.8.1	b3	All	All
Application	lsc	Bind	9.8.1	p1	All	All
Application	lsc	Bind	9.8.1	rc1	All	All
Application	lsc	Bind	9.8.2	b1	All	All
Application	lsc	Bind	9.8.2	rc1	All	All
Application	lsc	Bind	9.8.2	rc2	All	All
Application	lsc	Bind	9.8.3	All	All	All
Application	lsc	Bind	9.8.3	p1	All	All
Application	lsc	Bind	9.8.3	p2	All	All
Application	lsc	Bind	9.8.4	All	All	All
Application	lsc	Bind	9.8.5	All	All	All
Application	lsc	Bind	9.8.5	b1	All	All
Application	lsc	Bind	9.8.5	b2	All	All
Application	lsc	Bind	9.8.5	p1	All	All
Application	lsc	Bind	9.8.5	p2	All	All
Application	lsc	Bind	9.8.5	rc1	All	All
Application	lsc	Bind	9.8.5	rc2	All	All
Application	lsc	Bind	9.8.6	b1	All	All
Application	lsc	Bind	9.9.0	All	All	All
Application	lsc	Bind	9.9.0	a1	All	All
Application	lsc	Bind	9.9.0	a2	All	All
Application	lsc	Bind	9.9.0	a3	All	All
Application	lsc	Bind	9.9.0	b1	All	All
Application	lsc	Bind	9.9.0	b2	All	All
Application	lsc	Bind	9.9.0	rc1	All	All
Application	lsc	Bind	9.9.0	rc2	All	All
Application	lsc	Bind	9.9.0	rc3	All	All
Application	lsc	Bind	9.9.0	rc4	All	All
Application	lsc	Bind	9.9.1	All	All	All
Application	lsc	Bind	9.9.1	p1	All	All
Application	lsc	Bind	9.9.1	p2	All	All
Application	lsc	Bind	9.9.2	All	All	All
Application	lsc	Bind	9.9.3	All	All	All
Application	lsc	Bind	9.9.3	b1	All	All

Application	lsc	Bind	9.9.3	b2	All	All
Application	lsc	Bind	9.9.3	p1	All	All
Application	lsc	Bind	9.9.3	p2	All	All
Application	lsc	Bind	9.9.3	rc1	All	All
Application	lsc	Bind	9.9.3	rc2	All	All
Application	lsc	Bind	9.9.4	b1	All	All
Application	lsc	Bind	9.6	All	All	All
Application	lsc	Bind	9.6	r5_p1	All	All
Application	lsc	Bind	9.6	r6_b1	All	All
Application	lsc	Bind	9.6	r6_rc1	All	All
Application	lsc	Bind	9.6	r6_rc2	All	All
Application	lsc	Bind	9.6	r7_p1	All	All
Application	lsc	Bind	9.6	r7_p2	All	All
Application	lsc	Bind	9.6	r9_p1	All	All
Application	lsc	Bind	9.8.0	All	All	All
Application	lsc	Bind	9.8.0	a1	All	All
Application	lsc	Bind	9.8.0	b1	All	All
Application	lsc	Bind	9.8.0	p1	All	All
Application	lsc	Bind	9.8.0	p2	All	All
Application	lsc	Bind	9.8.0	p4	All	All
Application	lsc	Bind	9.8.0	rc1	All	All
Application	lsc	Bind	9.8.1	All	All	All
Application	lsc	Bind	9.8.1	b1	All	All
Application	lsc	Bind	9.8.1	b2	All	All
Application	lsc	Bind	9.8.1	b3	All	All
Application	lsc	Bind	9.8.1	p1	All	All
Application	lsc	Bind	9.8.1	rc1	All	All
Application	lsc	Bind	9.8.2	b1	All	All
Application	lsc	Bind	9.8.2	rc1	All	All
Application	lsc	Bind	9.8.2	rc2	All	All
Application	lsc	Bind	9.8.3	All	All	All
Application	lsc	Bind	9.8.3	p1	All	All
Application	lsc	Bind	9.8.3	p2	All	All
Application	lsc	Bind	9.8.4	All	All	All
Application	lsc	Bind	9.8.5	All	All	All
Application	lsc	Bind	9.8.5	All	All	All

Application	lsc	Bind	9.8.5	b1	All	All
Application	lsc	Bind	9.8.5	b2	All	All
Application	lsc	Bind	9.8.5	p1	All	All
Application	lsc	Bind	9.8.5	p2	All	All
Application	lsc	Bind	9.8.5	rc1	All	All
Application	lsc	Bind	9.8.5	rc2	All	All
Application	lsc	Bind	9.8.6	b1	All	All
Application	lsc	Bind	9.9.0	All	All	All
Application	lsc	Bind	9.9.0	a1	All	All
Application	lsc	Bind	9.9.0	a2	All	All
Application	lsc	Bind	9.9.0	a3	All	All
Application	lsc	Bind	9.9.0	b1	All	All
Application	lsc	Bind	9.9.0	b2	All	All
Application	lsc	Bind	9.9.0	rc1	All	All
Application	lsc	Bind	9.9.0	rc2	All	All
Application	lsc	Bind	9.9.0	rc3	All	All
Application	lsc	Bind	9.9.0	rc4	All	All
Application	lsc	Bind	9.9.1	All	All	All
Application	lsc	Bind	9.9.1	p1	All	All
Application	lsc	Bind	9.9.1	p2	All	All
Application	lsc	Bind	9.9.2	All	All	All
Application	lsc	Bind	9.9.3	All	All	All
Application	lsc	Bind	9.9.3	b1	All	All
Application	lsc	Bind	9.9.3	b2	All	All
Application	lsc	Bind	9.9.3	p1	All	All
Application	lsc	Bind	9.9.3	p2	All	All
Application	lsc	Bind	9.9.3	rc1	All	All
Application	lsc	Bind	9.9.3	rc2	All	All
Application	lsc	Bind	9.9.4	b1	All	All

References						
Reference						Source
CVE-2013-6230: FAQ and Supplemental Information Internet Systems Consortium Knowledge Base						CONF
The Slackware Linux Project: Slackware Security Advisories						SLACK
CVE-2013-6230: A Winsock API Bug Can Cause a Side-Effect Affecting BIND ACLs Internet Systems Consortium Knowledge Base						CONF
CVE Program record						CVE.C

No vendor comments have been submitted for this CVE.

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)