CVE-2014-8500

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

Summary

CVE	CVE-2014-8500
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-11 02:59:00 UTC
Updated	2017-01-03 02:59:00 UTC
Description	ISC BIND 9.0.x through 9.8.x, 9.9.0 through 9.9.6, and 9.10.0 through 9.10.1 does not limit delegation chaining, which allow

Risk And Classification

Problem Types: CWE-399

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	9.0.1	All	All	All
Application	Isc	Bind	9.1	All	All	All
Application	Isc	Bind	9.1.1	All	All	All
Application	Isc	Bind	9.1.2	All	All	All
Application	Isc	Bind	9.1.3	All	All	All
Application	Isc	Bind	9.10.0	All	All	All
Application	Isc	Bind	9.10.1	All	All	All
Application	Isc	Bind	9.2	All	All	All
Application	Isc	Bind	9.2.0	All	All	All
Application	Isc	Bind	9.2.1	All	All	All
Application	Isc	Bind	9.2.2	All	All	All
Application	Isc	Bind	9.2.3	All	All	All
Application	Isc	Bind	9.2.4	All	All	All
Application	Isc	Bind	9.2.5	All	All	All
Application	Isc	Bind	9.2.6	All	All	All
Application	Isc	Bind	9.2.7	All	All	All

Application	Isc	Bind	9.2.8	All	All	All
Application	Isc	Bind	9.2.9	All	All	All
Application	Isc	Bind	9.3	All	All	All
Application	Isc	Bind	9.3.0	All	All	All
Application	Isc	Bind	9.3.1	All	All	All
Application	Isc	Bind	9.3.2	All	All	All
Application	Isc	Bind	9.3.3	All	All	All
Application	Isc	Bind	9.3.4	All	All	All
Application	Isc	Bind	9.3.5	All	All	All
Application	Isc	Bind	9.3.6	All	All	All
Application	Isc	Bind	9.4	All	All	All
Application	Isc	Bind	9.4.0	All	All	All
Application	Isc	Bind	9.4.1	All	All	All
Application	Isc	Bind	9.4.2	All	All	All
Application	Isc	Bind	9.4.3	All	All	All
Application	Isc	Bind	9.5	All	All	All
Application	Isc	Bind	9.5.0	All	All	All
Application	Isc	Bind	9.5.1	All	All	All
Application	Isc	Bind	9.5.2	All	All	All
Application	Isc	Bind	9.5.3	All	All	All
Application	Isc	Bind	9.6.0	All	All	All
Application	Isc	Bind	9.6.1	All	All	All
Application	Isc	Bind	9.6.2	All	All	All
Application	Isc	Bind	9.6.3	All	All	All
Application	Isc	Bind	9.7.0	All	All	All
Application	Isc	Bind	9.7.1	All	All	All
Application	Isc	Bind	9.7.2	All	All	All
Application	Isc	Bind	9.7.3	All	All	All
Application	Isc	Bind	9.7.4	All	All	All
Application	Isc	Bind	9.7.5	All	All	All
Application	Isc	Bind	9.7.6	All	All	All
Application	Isc	Bind	9.7.7	All	All	All
Application	Isc	Bind	9.8.0	All	All	All
Application	Isc	Bind	9.8.1	All	All	All
Application	Isc	Bind	9.8.2	All	All	All

Application	Isc	Bind	9.8.3	All	All	All
Application	Isc	Bind	9.8.4	All	All	All
Application	Isc	Bind	9.8.5	All	All	All
Application	Isc	Bind	9.8.6	All	All	All
Application	Isc	Bind	9.9.0	All	All	All
Application	Isc	Bind	9.9.1	All	All	All
Application	Isc	Bind	9.9.2	All	All	All
Application	Isc	Bind	9.9.3	All	All	All
Application	Isc	Bind	9.9.4	All	All	All
Application	Isc	Bind	9.9.5	All	All	All
Application	Isc	Bind	9.9.6	All	All	All
Application	Isc	Bind	9.0	All	All	All
Application	Isc	Bind	9.0.1	All	All	All
Application	Isc	Bind	9.1	All	All	All
Application	Isc	Bind	9.1.1	All	All	All
Application	Isc	Bind	9.1.2	All	All	All
Application	Isc	Bind	9.1.3	All	All	All
Application	Isc	Bind	9.10.0	All	All	All
Application	Isc	Bind	9.10.1	All	All	All
Application	Isc	Bind	9.2	All	All	All
Application	Isc	Bind	9.2.0	All	All	All
Application	Isc	Bind	9.2.1	All	All	All
Application	Isc	Bind	9.2.2	All	All	All
Application	Isc	Bind	9.2.3	All	All	All
Application	Isc	Bind	9.2.4	All	All	All
Application	Isc	Bind	9.2.5	All	All	All
Application	Isc	Bind	9.2.6	All	All	All
Application	Isc	Bind	9.2.7	All	All	All
Application	Isc	Bind	9.2.8	All	All	All
Application	Isc	Bind	9.2.9	All	All	All
Application	Isc	Bind	9.3	All	All	All
Application	Isc	Bind	9.3.0	All	All	All
Application	Isc	Bind	9.3.1	All	All	All
Application	Isc	Bind	9.3.2	All	All	All
Application	Isc	Bind	9.3.3	All	All	All

Application	Isc	Bind	9.3.4	All	All	All
Application	Isc	Bind	9.3.5	All	All	All
Application	Isc	Bind	9.3.6	All	All	All
Application	Isc	Bind	9.4	All	All	All
Application	Isc	Bind	9.4.0	All	All	All
Application	Isc	Bind	9.4.1	All	All	All
Application	Isc	Bind	9.4.2	All	All	All
Application	Isc	Bind	9.4.3	All	All	All
Application	Isc	Bind	9.5	All	All	All
Application	Isc	Bind	9.5.0	All	All	All
Application	Isc	Bind	9.5.1	All	All	All
Application	Isc	Bind	9.5.2	All	All	All
Application	Isc	Bind	9.5.3	All	All	All
Application	Isc	Bind	9.6.0	All	All	All
Application	Isc	Bind	9.6.1	All	All	All
Application	Isc	Bind	9.6.2	All	All	All
Application	Isc	Bind	9.6.3	All	All	All
Application	Isc	Bind	9.7.0	All	All	All
Application	Isc	Bind	9.7.1	All	All	All
Application	Isc	Bind	9.7.2	All	All	All
Application	Isc	Bind	9.7.3	All	All	All
Application	Isc	Bind	9.7.4	All	All	All
Application	Isc	Bind	9.7.5	All	All	All
Application	Isc	Bind	9.7.6	All	All	All
Application	Isc	Bind	9.7.7	All	All	All
Application	Isc	Bind	9.8.0	All	All	All
Application	Isc	Bind	9.8.1	All	All	All
Application	Isc	Bind	9.8.2	All	All	All
Application	Isc	Bind	9.8.3	All	All	All
Application	Isc	Bind	9.8.4	All	All	All
Application	Isc	Bind	9.8.5	All	All	All
Application	Isc	Bind	9.8.6	All	All	All
Application	Isc	Bind	9.9.0	All	All	All
Application	Isc	Bind	9.9.1	All	All	All
Application	Isc	Bind	9.9.2	All	All	All
Application	Isc	Bind	9.9.3	All	All	All

Application	Isc	Bind	9.9.4	All	All	All
Application	Isc	Bind	9.9.5	All	All	All
Application	Isc	Bind	9.9.6	All	All	All

References

Reference
[security-announce] SUSE-SU-2015:0011-1: important: Security update for
'[security bulletin] HPSBUX03400 SSRT102211 rev.1 - HP-UX Running BIND, Remote Denial of Service (DoS' - MARC
Oracle Bulletin Board Update - January 2015
About the security content of OS X Server v5.0.3 - Apple Support
Red Hat Customer Portal
Multiples vulnérabilités dans plusieurs produits DNS
[security-announce] SUSE-SU-2015:0480-1: important: Security update for
[security-announce] SUSE-SU-2015:0096-1: important: Security update for
ISC BIND CVE-2014-8500 Remote Denial of Service Vulnerability
Debian -- Security Information -- DSA-3094-1 bind9
openSUSE-SU-2015:1250-1: moderate: Security update for bind
[security-announce] SUSE-SU-2015:0488-1: important: Security update for
CVE-2014-8500: A Defect in Delegation Handling Can Be Exploited to Crash BIND | Internet Systems Consortium Knowledge Base
About Secunia Research | Flexera
APPLE-SA-2015-09-16-4 OS X Server 5.0.3
ISC BIND Resolver Resource Consumption Flaw Lets Remote Users Deny Service - SecurityTracker
Vulnerability Note VU#264212 - Recursive DNS resolver implementations may follow referrals infinitely
'[security bulletin] HPSBUX03235 SSRT101750 rev.1 - HP-UX Running BIND, Remote Denial of Service (DoS' - MARC
Oracle VM Server for x86 Bulletin - July 2016
December 2014 ISC BIND Vulnerabilities in NetApp Products | NetApp Product Security
USN-2437-1: Bind vulnerability | Ubuntu
Mageia Advisory: MGASA-2014-0524 - Updated bind packages fix CVE-2014-8500
NetBSD-SA2015-002
BIND: Multiple Vulnerabilities (GLSA 201502-03) — Gentoo security
About Secunia Research | Flexera
Support / Security / Advisories / / MDVSA-2015:165 | Mandriva
2015-04 Security Bulletin: SRX Series: ISC BIND vulnerability denial of service in delegation handling (CVE-2014-8500) - Juniper Networks
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

15151 ISC BIND Denial of Service (DoS) Vulnerability (CVE-2014-8500)

Free CVE JSON API cve.report/api

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