CVE-2007-0493

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

Summary

CVE	CVE-2007-0493
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-01-25 20:28:00 UTC
Updated	2023-02-13 02:17:00 UTC
Description	Use-after-free vulnerability in ISC BIND 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: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	9.4.0	All	All	All
Application	Isc	Bind	9.4.0	rc1	All	All
Application	Isc	Bind	9.5.0	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	9.4.0	All	All	All
Application	Isc	Bind	9.4.0	rc1	All	All
Application	Isc	Bind	9.5.0	All	All	All

References

Reference
2007-0005
FreeBSD update for bind - Advisories - Secunia

Ubuntu update for bind - 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

Red Hat Customer Portal

Webmail - OVH

Trustix update for bind and ed - Advisories - Secunia

SecurityTracker.com Archives - BIND Memory Deference Bug Lets Remote Users Crash the Name Server

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[Full-disclosure] BIND remote exploit (low severity) [Fwd: Internet Systems Consortium Security Advisory.]

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

HP Tru64 UNIX Multiple SSL and BIND Vulnerabilities - Advisories - Secunia

Gentoo Linux Documentation -- BIND: Denial of Service

230003 – (CVE-2007-0493) CVE-2007-0493 bind use-after-free

rhn.redhat.com | Red Hat Support

Document Display | HPE Support Center

Advisories | Mandriva

rPath update for bind and bind-utils - Advisories - Secunia

SecurityFocus

Fedora update for bind - Advisories - Secunia

SUSE update for bind - Advisories - Secunia

SSRT061273

NetBSD-SA2007-003

The Slackware Linux Project: Slackware Security Advisories

Fedora update for bind - 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

Cisco PIX Connection Security Security Advisories

OpenPKG Corporation: Security: Security Advisories
HP Insight Management Agents SSL Vulnerabilities - Advisories - Secunia
'Internet Systems Consortium Security Advisory.' - MARC
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)
SSRT071304
ISC has a new website | Internet Systems Consortium
access.redhat.com | CVE-2007-0493
Mandriva update for bind - Advisories - Secunia
Repository / Oval Repository
ISC BIND Remote Fetch Context Denial of Service Vulnerability
About Security Update 2007-005
Slackware update for bind - Advisories - Secunia
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-01-29	Joshua Bressers	Not vulnerable. This issue did not affect the versions of ISC BIND as shipped with Red Hat I

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 registred 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**