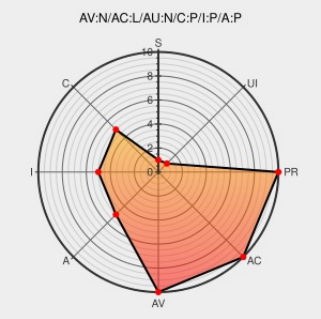
CVE-2002-0651

Published on: 07/03/2002 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:03 PM UTC

CVE-2002-0651

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Bind from Isc contain the following vulnerability:

Buffer overflow in the DNS resolver code used in libc, glibc, and libbind, as derived from ISC BIND, allows remote malicious DNS servers to cause a denial of service and possibly execute arbitrary code via the stub resolvers.

CVE-2002-0651 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Multiple Vendor libc DNS Resolver Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 5100
Pine Digital Security	www.pine.nl text/html	>> MISC www.pine.nl/advisories/pine-cert-20020601.txt
CERT Advisory CA-2002-19 Buffer Overflows in Multiple DNS Resolver Libraries	Patch Third Party Advisory US Government Resource www.cert.org text/html	CERT CA-2002-19
Advisories - Mandriva Linux	frontal2.mandriva.com text/html	MANDRAKE MDKSA-2002:038
redhat.com | Red Hat Support	www.redhat.com	REDHAT RHSA-

	text/html	2002:133
	ftp.NetBSD.ORG text/plain	NETBSD NetBSD-SA2002-006
No Description Provided	ftp.caldera.com Inactive Link Not Archived	CALDERA CSSA-2002-SCO.37
No Description Provided	patches.sgi.com Inactive Link Not Archived	SGI 20020701-01-I
redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2002:167
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:4190
CERT/CC Vulnerability Note VU#803539	US Government Resource www.kb.cert.org text/html	CERT-VN VU#803539
redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2003:154
redhat.com | Red Hat Support	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2002:139
ISS X-Force Database: dns-resolver-lib-bo (9432): Multiple vendor DNS resolver library buffer overflow	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	XF dns-resolver-lib-bo(9432)
Neohapsis Archives - IBM AIX lists - Re: Security - From aixserv_at_austin.ibm.com	web.archive.org text/html Inactive Link Not Archived	AIXAPAR IY32746
'FreeBSD Security Advisory FreeBSD-SA-02:28.resolv' - MARC	marc.info text/html	FREEBSD FreeBSD-SA-02:28
Neohapsis Archives - EnGarde Linux - [ESA-20020724-018] Buffer overflow in BIND4-derived resolver code. - From engarde-announce-admins_at_guardiandigital.com	web.archive.org text/html Inactive Link Not Archived	ENGARDE ESA-20020724-018
No Description Provided	www.linux-mandrake.com Inactive Link Not Archived	MANDRAKE MDKSA-2002:043
No Description Provided	ftp.caldera.com Inactive Link Not Archived	CALDERA CSSA-2002-SCO.39
redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2002:119
'Remote buffer overflow in resolver code of libc' - MARC	marc.info text/html	BUGTRAQ 20020626 Remote buffer overflow in resolver code of libc
No Description Provided	web.archive.org text/html Inactive Link Not Archived	CONECTIVA CLSA-2002:507
No Description Provided	web.archive.org text/html Inactive Link Not Archived	NTBUGTRAQ 20020703 Buffer overflow and DoS i BIND

'[OpenPKG-SA-2002.006] OpenPKG Security Advisory (bind)' - MARC	marc.info text/html	BUGTRAQ 20020704 [OpenPKG-SA-2002.006] OpenPKG Security Advisory (bind)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:isc:bind:9.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.4.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→