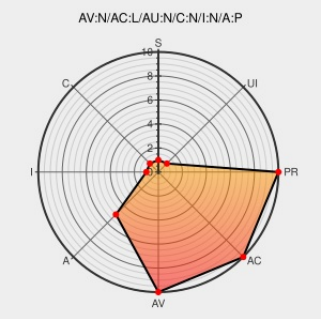
# CVE-2002-1221

Published on: 11/29/2002 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:01 PM UTC

## CVE-2002-1221

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




Certain versions of Freebsd from Freebsd contain the following vulnerability:

BIND 8.x through 8.3.3 allows remote attackers to cause a denial of service (crash) via SIG RR elements with invalid expiry times, which are removed from the internal BIND database and later cause a null dereference.

CVE-2002-1221 has been assigned by cve@mitre.org to track the vulnerability

### CVSS2 Score: 5 - MEDIUM

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

### CVE References

| Description | Tags | Link |
|---|---|---|
| Repository / Oval Repository | oval.cisecurity.org<br>text/html | OVAL oval:org.mitre.oval:def:2094 |
| CERT Advisory CA-2002-31 Multiple Vulnerabilities in BIND | US Government Resource<br>www.cert.org<br>text/html | CERT CA-2002-31 |
| CERT/CC Vulnerability Note VU#581682 | US Government Resource<br>www.kb.cert.org<br>text/html | CERT-VN VU#581682 |
| No Description Provided | www.linux-mandrake.com<br>Inactive Link Not Archived | MANDRAKE MDKSA-2002:077 |
| Internet Software Consortium: BIND Vulnerabilities | Patch<br>Vendor Advisory | CONFIRM www.isc.org/products/BIND/bind-security.html |

| | | |
|---|---|---|
| | web.archive.org<br>text/html<br>Inactive Link Not Archived | |
| Security Update 2002-11-21 is available | lists.apple.com<br>text/html | APPLE 2002-11-21 |
| IBM X-Force Exchange | exchange.xforce.ibmcloud.com<br>text/html | XF bind-null-dereference-dos(10333) |
| '[Fwd: Notice of serious vulnerabilities in ISC BIND 4 & 8]' - MARC | marc.info<br>text/html | BUGTRAQ 20021112 [Fwd: Notice of serious vulnerabilities in ISC BIND 4 & 8] |
| No Description Provided | online.securityfocus.com<br>Inactive Link Not Archived | COMPAQ SSRT2408 |
| ISS: Security Center: X-Force Alerts and Advisories | Patch<br>Vendor Advisory<br>web.archive.org<br>text/html<br>Inactive Link Not Archived | ISS 20021112 Multiple Remote Vulnerabilities in BIND4 and BIND8 |
| 'TSLSA-2002-0076 - bind' - MARC | marc.info<br>text/html | BUGTRAQ 20021118 TSLSA-2002-0076 - bind |
| Home - Conectiva | distro.conectiva.com.br<br>text/html | CONECTIVA CLA-2002:546 |
| ISC BIND 8 Invalid Expiry Time Denial Of Service Vulnerability | cve.report (archive)<br>text/html | BID 6159 |
| N-013: ISC Remote Vulnerabilities in BIND4 and BIND8 | web.archive.org<br>text/html<br>Inactive Link Not Archived | CIAC N-013 |
| SecurityFocus HOME Mailing List: BugTraq | web.archive.org<br>text/html<br>Inactive Link Not Archived | BUGTRAQ 20021115 [OpenPKG-SA-2002.011] OpenPKG Security Advisory (bind, bind8) |
| Debian -- Security Information -- DSA-196-1 bind | www.debian.org<br>Depreciated Link<br>text/html | DEBIAN DSA-196 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Freebsd | Freebsd | 4.4 | All | All | All |
| Operating System | Freebsd | Freebsd | 4.5 | All | All | All |
| Operating System | Freebsd | Freebsd | 4.6 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Freebsd | Freebsd | 4.7 | All | All | All |
| Operating System | Freebsd | Freebsd | 4.4 | All | All | All |
| Operating System | Freebsd | Freebsd | 4.5 | All | All | All |
| Operating System | Freebsd | Freebsd | 4.6 | All | All | All |
| Operating System | Freebsd | Freebsd | 4.7 | All | All | All |
| Application | Isc | Bind | 8.1 | All | All | All |
| Application | Isc | Bind | 8.1.1 | All | All | All |
| Application | Isc | Bind | 8.1.2 | All | All | All |
| Application | Isc | Bind | 8.2 | All | All | All |
| Application | Isc | Bind | 8.2.1 | All | All | All |
| Application | Isc | Bind | 8.2.2 | All | All | All |
| Application | Isc | Bind | 8.2.3 | All | All | All |
| Application | Isc | Bind | 8.2.4 | All | All | All |
| Application | Isc | Bind | 8.2.5 | All | All | All |
| Application | Isc | Bind | 8.2.6 | All | All | All |
| Application | Isc | Bind | 8.3.0 | All | All | All |
| Application | Isc | Bind | 8.3.1 | All | All | All |
| Application | Isc | Bind | 8.3.2 | All | All | All |
| Application | Isc | Bind | 8.3.3 | All | All | All |
| Application | Isc | Bind | 8.1 | All | All | All |
| Application | Isc | Bind | 8.1.1 | All | All | All |
| Application | Isc | Bind | 8.1.2 | All | All | All |
| Application | Isc | Bind | 8.2 | All | All | All |
| Application | Isc | Bind | 8.2.1 | All | All | All |
| Application | Isc | Bind | 8.2.2 | All | All | All |
| Application | Isc | Bind | 8.2.3 | All | All | All |
| Application | Isc | Bind | 8.2.4 | All | All | All |
| Application | Isc | Bind | 8.2.5 | All | All | All |
| Application | Isc | Bind | 8.2.6 | All | All | All |
| Application | Isc | Bind | 8.3.0 | All | All | All |
| Application | Isc | Bind | 8.3.1 | All | All | All |
| Application | Isc | Bind | 8.3.2 | All | All | All |
| Application | Isc | Bind | 8.3.3 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Openbsd | Openbsd | 3.0 | All | All | All |
| Operating System | Openbsd | Openbsd | 3.1 | All | All | All |
| Operating System | Openbsd | Openbsd | 3.2 | All | All | All |
| Operating System | Openbsd | Openbsd | 3.0 | All | All | All |
| Operating System | Openbsd | Openbsd | 3.1 | All | All | All |
| Operating System | Openbsd | Openbsd | 3.2 | All | All | All |

cpe:2.3:o:freebsd:freebsd:4.4:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:4.5:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:4.6:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:4.7:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:4.4:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:4.5:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:4.6:*:*:*:*:*:*:*:

cpe:2.3:o:freebsd:freebsd:4.7:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.3.3:*:*:*:*:*:*:*:

cpe:2.3:o:openbsd:openbsd:3.0:*:*:*:*:*:*:*:

cpe:2.3:o:openbsd:openbsd:3.1:*:*:*:*:*:*:*:

cpe:2.3:o:openbsd:openbsd:3.2:*:*:*:*:*:*:*:

cpe:2.3:o:openbsd:openbsd:3.0:*:*:*:*:*:*:*:

cpe:2.3:o:openbsd:openbsd:3.1:*:*:*:*:*:*:*:

cpe:2.3:o:openbsd:openbsd:3.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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