# CVE-2012-1033

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2012-1033 |
| **State** | PUBLISHED |
| **Assigner** | mitre |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2012-02-08 20:55:01 UTC |
| **Updated** | 2026-04-29 01:13:23 UTC |
| **Description** | The resolver in ISC BIND 9 through 9.8.1-P1 overwrites cached server names and TTL values in NS records during the pro |

## Risk And Classification

**Primary CVSS:** v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:P/A:N

**Problem Types:** NVD-CWE-Other | n/a

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:L/Au:N/C:N/I:P/A:N

## 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 | 9.2 | 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 | 9.2.2 | p3 | 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 | 9.3 | 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 | 9.4 | All | All | All |
| Application | Isc | Bind | 9.4.0 | All | All | All |
| Application | Isc | Bind | 9.4.0 | rc1 | All | All |
| Application | Isc | Bind | 9.4.1 | All | All | All |
| Application | Isc | Bind | 9.4.2 | All | All | All |
| Application | Isc | Bind | 9.4.3 | All | All | All |
| Application | Isc | Bind | 9.4.3 | rc1 | All | All |
| Application | Isc | Bind | 9.5 | All | All | All |
| Application | Isc | Bind | 9.5.0 | All | All | All |
| Application | Isc | Bind | 9.5.0 | rc1 | All | All |
| Application | Isc | Bind | 9.5.1 | All | All | All |
| Application | Isc | Bind | 9.5.1 | rc1 | All | All |
| Application | Isc | Bind | 9.5.1 | rc2 | All | All |
| Application | Isc | Bind | 9.6.0 | All | All | All |
| Application | Isc | Bind | 9.6.0 | p1 | All | All |
| Application | Isc | Bind | 9.6.0 | rc1 | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Isc | Bind | 9.6.0 | rc2 | All | All |
| Application | Isc | Bind | 9.7.0 | All | All | All |
| Application | Isc | Bind | 9.7.0 | b1 | All | All |
| Application | Isc | Bind | 9.7.0 | p1 | All | All |
| Application | Isc | Bind | 9.7.0 | p2 | All | All |
| Application | Isc | Bind | 9.7.0 | rc1 | All | All |
| Application | Isc | Bind | 9.7.0 | rc2 | All | All |
| Application | Isc | Bind | 9.7.1 | All | All | All |
| Application | Isc | Bind | 9.7.1 | p1 | All | All |
| Application | Isc | Bind | 9.7.1 | p2 | All | All |
| Application | Isc | Bind | 9.7.1 | rc1 | All | All |
| Application | Isc | Bind | 9.7.2 | All | All | All |
| Application | Isc | Bind | 9.7.2 | p1 | All | All |
| Application | Isc | Bind | 9.7.2 | p2 | All | All |
| Application | Isc | Bind | 9.7.2 | p3 | All | All |
| Application | Isc | Bind | 9.7.2 | rc1 | All | All |
| Application | Isc | Bind | 9.7.3 | All | All | All |
| Application | Isc | Bind | 9.7.3 | b1 | All | All |
| Application | Isc | Bind | 9.7.3 | p1 | All | All |
| Application | Isc | Bind | 9.7.3 | rc1 | All | All |
| Application | Isc | Bind | 9.7.4 | All | All | All |
| Application | Isc | Bind | 9.7.4 | b1 | 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 | Isc | Bind | 9.8.1 | b2 | All | All |
| Application | Isc | Bind | 9.8.1 | b3 | All | All |
| Application | Isc | Bind | 9.8.1 | p1 | All | All |
| Application | Isc | Bind | 9.8.1 | rc1 | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Na | N/a | affected n/a | Not specified |

## References

| Reference | Source |
|---|---|
| Vulnerability Note VU#542123 - ISC BIND 9 resolver cache vulnerability | af854a3a-212 |
| hermes.opensuse.org/messages/15136456 | af854a3a-212 |
| hermes.opensuse.org/messages/15136477 | af854a3a-212 |
| ISC BIND Cache Update Policy Can Be Bypassed to Allow Revoked Domain Names to Remain Resolvable - SecurityTracker | af854a3a-212 |
| ISC BIND CVE-2012-1033 Security Bypass Vulnerability | af854a3a-212 |
| Ghost Domain Names: Revoked Yet Still Resolvable \| Internet Systems Consortium | af854a3a-212 |
| IBM X-Force Exchange | af854a3a-212 |
| '[security bulletin] HPSBUX02835 SSRT100763 rev.1 - HP-UX Running BIND, Remote Domain Name Revalidati' - MARC | af854a3a-212 |
| Security Alerts - Secunia | af854a3a-212 |
| Red Hat Customer Portal | af854a3a-212 |
| osvdb.org/78916 | af854a3a-212 |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.