1 Release Notes for BIND Version 9.12.2rc1

1.1 Introduction

This document summarizes changes since the last production release on the BIND 9.12 branch. Please see the CHANGES for a further list of bug fixes and other changes.

1.2 Download

The latest versions of BIND 9 software can always be found at http://www.isc.org/downloads/. There you will find additional information about each release, source code, and pre-compiled versions for Microsoft Windows operating systems.

1.3 Security Fixes

- When recursion is enabled but the allow-recursion and allow-query-cache ACLs are not specified, they should be limited to local networks, but they were inadvertently set to match the default allow-query, thus allowing remote queries. This flaw is disclosed in CVE-2018-5738. [GL #309]

- The serve-stale feature could cause an assertion failure in rbtdb.c even when stale-answer-enable was false. The simultaneous use of stale cache records and NSEC aggressive negative caching could trigger a recursion loop in the named process. This flaw is disclosed in CVE-2018-5737. [GL #185]

- A bug in zone database reference counting could lead to a crash when multiple versions of a slave zone were transferred from a master in close succession. This flaw is disclosed in CVE-2018-5736. [GL #134]

1.4 New Features

- update-policy rules that otherwise ignore the name field now require that it be set to "." to ensure that any type list present is properly interpreted. Previously, if the name field was omitted from the rule declaration but a type list was present, it wouldn’t be interpreted as expected.

- named now supports the “root key sentinel” mechanism. This enables validating resolvers to indicate which trust anchors are configured for the root, so that information about root key rollover status can be gathered. To disable this feature, add root-key-sentinel no; to named.conf. [GL #37]

- Add the ability to not return a DNS COOKIE option when one is present in the request. To prevent a cookie being returned add ‘answer-cookie no;’ to named.conf. [GL #173]

  answer-cookie is only available as a temporary measure, for use when named shares an IP address with other servers that do not yet support DNS COOKIE. A mismatch between servers on the same address is not expected to cause operational problems, but the option to disable COOKIE responses so that all servers have the same behavior is provided out of an abundance of caution. DNS COOKIE is an important security mechanism and should not be disabled unless absolutely necessary. The answer-cookie option is obsolete as of BIND 9.13.

1.5 Feature Changes

- named will now log a warning if the old root DNSSEC key is explicitly configured and has not been updated. [RT #43670]

- BIND now can be compiled against libidn2 library to add IDNA2008 support. Previously BIND only supported IDNA2003 using (now obsolete) idnkit-1 library.

- dig +noidnin can be used to disable IDN processing on the input domain name, when BIND is compiled with IDN support.
1.6  Bug Fixes

- When answering authoritative queries, named does not return the target of a cross-zone CNAME between two locally served zones; this prevents accidental cache poisoning. This same restriction was incorrectly applied to recursive queries as well; this has been fixed. [RT #47078]

- named could crash when acting as a slave for a catalog zone if zone contained a master definition without an IP address. [RT #45999]

- named could crash due to a race condition when rolling dnstap log files. [RT #46942]

- rndc reload could cause named to leak memory if it was invoked before the zone loading actions from a previous rndc reload command were completed. [RT #47076]

- named could crash when rolling a dnstap log file. [RT #46942]

1.7  License

BIND is open source software licenced under the terms of the Mozilla Public License, version 2.0 (see the LICENSE file for the full text).

The license requires that if you make changes to BIND and distribute them outside your organization, those changes must be published under the same license. It does not require that you publish or disclose anything other than the changes you have made to our software. This requirement does not affect anyone who is using BIND, with or without modifications, without redistributing it, nor anyone redistributing BIND without changes.

Those wishing to discuss license compliance may contact ISC at https://www.isc.org/mission/contact/.

1.8  End of Life

The end-of-life date for BIND 9.12 has not yet been determined. However, it is not intended to be an Extended Support Version (ESV) branch; accordingly, support will end after the next stable branch (9.14) becomes available. Those needing a longer-lived branch are encouraged to use the current ESV, BIND 9.11, which will be supported until December 2021. See https://www.isc.org/downloads/software-support-policy/ for details of ISC’s software support policy.

1.9  Thank You

Thank you to everyone who assisted us in making this release possible. If you would like to contribute to ISC to assist us in continuing to make quality open source software, please visit our donations page at http://www.isc.org/donate/.