1 Release Notes for BIND Version 9.12.4rc1

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

- **named** could crash during recursive processing of DNAME records when **deny-answer-aliases** was in use. This flaw is disclosed in CVE-2018-5740. [GL #387]
- 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]
- Code change #4964, intended to prevent double signatures when deleting an inactive zone DNSKEY in some situations, introduced a new problem during zone processing in which some delegation glue RRsets are incorrectly identified as needing RRSIGs, which are then created for them using the current active ZSK for the zone. In some, but not all cases, the newly-signed RRsets are added to the zone's NSEC/NSEC3 chain, but incompletely -- this can result in a broken chain, affecting validation of proof of nonexistence for records in the zone. [GL #771]
- **named** could crash if it managed a DNSSEC security root with **managed-keys** and the authoritative zone rolled the key to an algorithm not supported by BIND 9. This flaw is disclosed in CVE-2018-5745. [GL #780]
- **named** leaked memory when processing a request with multiple Key Tag EDNS options present. ISC would like to thank Toshifumi Sakaguchi for bringing this to our attention. This flaw is disclosed in CVE-2018-5744. [GL #772]
- Zone transfer controls for writable DLZ zones were not effective as the **allowzonexfr** method was not being called for such zones. This flaw is disclosed in CVE-2019-6465. [GL #790]

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 no is only intended 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.

- Two new update policy rule types have been added **krb5-selfsub** and **ms-selfsub** which allow machines with Kerberos principals to update the name space at or below the machine names identified in the respective principals.

- The new configure option **--enable-fips-mode** can be used to make BIND enable and enforce FIPS mode in the OpenSSL library. When compiled with such option the BIND will refuse to run if FIPS mode can't be enabled, thus this option must be only enabled for the systems where FIPS mode is available.

1.5 Feature Changes

- 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.

- The **rndc nta** command could not differentiate between views of the same name but different class; this has been corrected with the addition of a **-class** option. [GL #105]

- When compiled with IDN support, the **dig** and the **nslookup** commands now disable IDN processing when the standard output is not a tty (e.g. not used by human). The command line options +idnin and +idnout need to be used to enable IDN processing when **dig** or **nslookup** is used from the shell scripts.

1.6 Bug Fixes

- When a negative trust anchor was added to multiple views using **rndc nta**, the text returned via **rndc** was incorrectly truncated after the first line, making it appear that only one NTA had been added. This has been fixed. [GL #105]

- **named** now rejects excessively large incremental (IXFR) zone transfers in order to prevent possible corruption of journal files which could cause **named** to abort when loading zones. [GL #339]

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/.