1 Release Notes for BIND Version 9.11.6

1.1 Introduction

This document summarizes changes since the last production release on the BIND 9.11 (Extended Support Version) branch. Please see the `CHANGES` file 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 License Change

With the release of BIND 9.11.0, ISC changed to the open source license for BIND from the ISC license to the Mozilla Public License (MPL 2.0).

The MPL-2.0 license requires that if you make changes to licensed software (e.g. BIND) and distribute them outside your organization, that you publish those changes under that same license. It does not require that you publish or disclose anything other than the changes you made to our software.

This requirement will not affect anyone who is using BIND, with or without modifications, without redistributing it, nor anyone redistributing it without changes. Therefore, this change will be without consequence for most individuals and organizations who are using BIND.

Those unsure whether or not the license change affects their use of BIND, or who wish to discuss how to comply with the license may contact ISC at https://www.isc.org/mission/contact/.

1.4 Legacy Windows No Longer Supported

As of BIND 9.11.2, Windows XP and Windows 2003 are no longer supported platforms for BIND; "XP" binaries are no longer available for download from ISC.

1.5 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]
- 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]

1.6 New Features

- **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`.
- Added the ability not to 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.

1.7 Removed Features

- **named** will now log a warning if the old BIND now can be compiled against libidn2 library to add IDNA2008 support. Previously BIND only supported IDNA2003 using (now obsolete) idnkit-1 library.

1.8 Feature Changes

- **dig +noidnin** can be used to disable IDN processing on the input domain name, when BIND is compiled with IDN support.
- Multiple **cookie-secret** clause are now supported. The first **cookie-secret** in `named.conf` is used to generate new server cookies. Any others are used to accept old server cookies or those generated by other servers using the matching **cookie-secret**.
- 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.
- By default, BIND now uses the random number generation functions in the cryptographic library (i.e., OpenSSL or a PKCS#11 provider) as a source of high-quality randomness rather than `/dev/random`. This is suitable for virtual machine environments, which may have limited entropy pools and lack hardware random number generators.

  This can be overridden by specifying another entropy source via the **random-device** option in `named.conf`, or via the **-r** command line option. However, for functions requiring full cryptographic strength, such as DNSSEC key generation, this *cannot* be overridden. In particular, the **-r** command line option no longer has any effect on **dnssec-keygen**.

  This can be disabled by building with **configure --disable-crypto-rand**, in which case `/dev/random` will be the default entropy source. [RT #31459] [RT #46047]

1.9 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]

- **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]

1.10 End of Life

BIND 9.11 (Extended Support Version) will be supported until at least December, 2021. See https://www.isc.org/dow
support-policy/ for details of ISC's software support policy.

1.11 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/.