

1 Release Notes for BIND Version 9.11.3

1.1 Introduction

This document summarizes changes since the last production release on the BIND 9.11 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 New DNSSEC Root Key

ICANN is in the process of introducing a new Key Signing Key (KSK) for the global root zone. BIND has multiple methods for managing DNSSEC trust anchors, with somewhat different behaviors. If the root key is configured using the **managed-keys** statement, or if the pre-configured root key is enabled by using **dnssec-validation auto**, then BIND can keep keys up to date automatically. Servers configured in this way should have begun the process of rolling to the new key when it was published in the root zone in July 2017. However, keys configured using the **trusted-keys** statement are not automatically maintained. If your server is performing DNSSEC validation and is configured using **trusted-keys**, you are advised to change your configuration before the root zone begins signing with the new KSK. This is currently scheduled for October 11, 2017.

This release includes an updated version of the `bind.keys` file containing the new root key. This file can also be downloaded from <https://www.isc.org/bind-keys>.

1.4 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/>.

1.5 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.

1.6 Security Fixes

- An error in TSIG handling could permit unauthorized zone transfers or zone updates. These flaws are disclosed in CVE-2017-3142 and CVE-2017-3143. [RT #45383]
- The BIND installer on Windows used an unquoted service path, which can enable privilege escalation. This flaw is disclosed in CVE-2017-3141. [RT #45229]
- With certain RPZ configurations, a response with TTL 0 could cause **named** to go into an infinite query loop. This flaw is disclosed in CVE-2017-3140. [RT #45181]
- Addresses could be referenced after being freed during resolver processing, causing an assertion failure. The chances of this happening were remote, but the introduction of a delay in resolution increased them. This bug is disclosed in CVE-2017-3145. [RT #46839]

- 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. If the name field was omitted from the rule declaration and a type list was present it wouldn't be interpreted as expected.

1.7 Removed Features

- The ISC DNSSEC Lookaside Validation (DLV) service has been shut down; all DLV records in the `dlv.isc.org` zone have been removed. References to the service have been removed from BIND documentation. Lookaside validation is no longer used by default by `delv`. The DLV key has been removed from `bind.keys`. Setting `dnssec-lookaside` to `auto` or to use `dlv.isc.org` as a trust anchor results in a warning being issued.
- `named` will now log a warning if the old root DNSSEC key is explicitly configured and has not been updated. [RT #43670]

1.8 Protocol Changes

- BIND can now use the Ed25519 and Ed448 Edwards Curve DNSSEC signing algorithms described in RFC 8080. Note, however, that these algorithms must be supported in OpenSSL; currently they are only available in the development branch of OpenSSL at <https://github.com/openssl/openssl>. [RT #44696]
- When parsing DNS messages, EDNS KEY TAG options are checked for correctness. When printing messages (for example, in `dig`), EDNS KEY TAG options are printed in readable format.

1.9 Feature Changes

- `named` will no longer start or accept reconfiguration if `managed-keys` or `dnssec-validation auto` are in use and the managed-keys directory (specified by `managed-keys-directory`, and defaulting to the working directory if not specified), is not writable by the effective user ID. [RT #46077]
- Previously, `update-policy local`; accepted updates from any source so long as they were signed by the locally-generated session key. This has been further restricted; updates are now only accepted from locally configured addresses. [RT #45492]
- `dig +ednsopt` now accepts the names for EDNS options in addition to numeric values. For example, an EDNS Client-Subnet option could be sent using `dig +ednsopt=ecs:....`. Thanks to John Worley of Secure64 for the contribution. [RT #44461]
- Threads in `named` are now set to human-readable names to assist debugging on operating systems that support that. Threads will have names such as "isc-timer", "isc-sockmgr", "isc-worker0001", and so on. This will affect the reporting of subsidiary thread names in `ps` and `top`, but not the main thread. [RT #43234]
- DiG now warns about .local queries which are reserved for Multicast DNS. [RT #44783]

1.10 Bug Fixes

- Attempting to validate improperly unsigned CNAME responses from secure zones could cause a validator loop. This caused a delay in returning SERVFAIL and also increased the chances of encountering the crash bug described in CVE-2017-3145. [RT #46839]
- When `named` was reconfigured, failure of some zones to load correctly could leave the system in an inconsistent state; while generally harmless, this could lead to a crash later when using `rndc addzone`. Reconfiguration changes are now fully rolled back in the event of failure. [RT #45841]
- Fixed a bug that was introduced in an earlier development release which caused multi-packet AXFR and IXFR messages to fail validation if not all packets contained TSIG records; this caused interoperability problems with some other DNS implementations. [RT #45509]
- Reloading or reconfiguring `named` could fail on some platforms when LMDB was in use. [RT #45203]

- Due to some incorrectly deleted code, when BIND was built with LMDB, zones that were deleted via **rndc delzone** were removed from the running server but were not removed from the new zone database, so that deletion did not persist after a server restart. This has been corrected. [RT #45185]
- Semicolons are no longer escaped when printing CAA and URI records. This may break applications that depend on the presence of the backslash before the semicolon. [RT #45216]
- AD could be set on truncated answer with no records present in the answer and authority sections. [RT #45140]
- Some header files included `<isc/util.h>` incorrectly as it pollutes with namespace with non `ISC_` macros and this should only be done by explicitly including `<isc/util.h>`. This has been corrected. Some code may depend on `<isc/util.h>` being implicitly included via other header files. Such code should explicitly include `<isc/util.h>`.
- Zones created with **rndc addzone** could temporarily fail to inherit the **allow-transfer** ACL set in the **options** section of `named.conf`. [RT #46603]
- **named** failed to properly determine whether there were active KSK and ZSK keys for an algorithm when **update-check-ksk** was true (which is the default setting). This could leave records unsigned when rolling keys. [RT #46743] [RT #46754] [RT #46774]

1.11 End of Life

The end of life for BIND 9.11 is yet to be determined but will not be before BIND 9.13.0 has been released for 6 months. <https://www.isc.org/downloads/software-support-policy/>

1.12 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/>.