1 Release Notes for BIND Version 9.11.3-S1

1.1 Introduction

This is a release of the BIND 9.11 Supported Preview Edition, a special feature preview branch of BIND which is available to ISC customers.

This document summarizes significant changes since the last production release on the BIND 9.11 (Extended Support Version) branch. Please see the file CHANGES for a complete list of bug fixes and other changes, or CHANGES.SE for a list of changes that have been applied specifically to the Supported Preview edition.

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 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.

1.4 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.

1.5 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]

1.6 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.

- **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]
- Query logging now includes the ECS option, if one was present in the query, in the format "[ECS `address/source/scope`]".

1.7 New Features

- This release introduces support for the EDNS CLIENT-SUBNET (ECS) option in recursive servers.
  - ECS options are generated when sending recursive queries to zones listed in `ecs-zones`.
  - ECS options from the client are forwarded when sending queries to whitelisted domains if the client is in allowed by the `ecs-forward` ACL, or when the source prefix length is 0
  - ECS options are never sent for DNS infrastructure types (i.e., NS, SOA, DNSKEY, etc) as these are presumed to be of global scope. ECS queries can be further restricted to a specific set of query types by using the `ecs-types` option.
  - ECS options are sent using a default source prefix length of 24 for IPv4 queries and 56 for IPv6 queries. These defaults can be reduced to lower values by using `ecs-bits`, or on a per-domain basis in the `ecs-zones` option.
  - Servers that do not support ECS can be blacklisted using **server IPADDR { ecs no; };**
  - The dns_db API and the red-black tree database implementation have been updated to allow storage and retrieval of data tagged with ECS information.

  See the ARM for more details of these options.
- The EDNS CLIENT SUBNET (ECS) option is also experimentally supported for authoritative servers: if an authoritative query contains an ECS option, then ACLs containing `geoip` or `ecs` elements can be matched against the address or prefix encoded in the option. This can be used to select a view for the query, so that different answers can be provided depending on the client network. Note, however, that this authoritative support is based on an outdated version of the ECS specification; in its current form it may be useful for testing, but is not recommended for production use. Thanks to Vincent Bernat for the contribution. [RT #36781]
- Added support for the EDNS TCP Keepalive option (RFC 7828); this allows negotiation of longer-lived TCP sessions to reduce the overhead of setting up TCP for individual queries. [RT #42126]
- Added support for the EDNS Padding option (RFC 7830), which obfuscates packet size analysis when DNS queries are sent over an encrypted channel. [RT #42094]
- **dnstap** logfiles can now be configured to automatically roll when they reach a specified size. If **dnstap-output** is configured with mode `file`, then it can take optional **size** and **versions** key-value arguments to set the logfile rolling parameters. (These have the same semantics as the corresponding options in a **logging** channel statement.) [RT #44502]
- The `print-time` option in the `logging` configuration can now take arguments **local**, **iso8601** or **iso8601-utc** to indicate the format in which the date and time should be logged. For backward compatibility, **yes** is a synonym for **local**. [RT #42585]
- New classification options have been added for response rate limiting (RRL):
  - Multiple `rate-limit` statements can now be configured, each defined by a specific `domain`. This allows different rate limiting options to be applied for different namespaces.
  - Each rate limiter may be configured with up to five `responses-per-second` options, with the value selected depending on the size of the response or the ratio of the response size to the query size (i.e., the amplification factor). For example, responses could rate limited to 10 per second in general, but only 2 per second for responses larger than 1100 bytes.

1.8 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]
- The Response Policy Zone (RPZ) implementation has been substantially refactored: updates to the RPZ summary database are no longer directly performed by the zone database but by a separate function that is called when a policy zone is updated. This improves both performance and reliability when policy zones receive frequent updates. Summary database updates can be rate-limited by using the **min-update-interval** option in a **response-policy** statement. [RT #43449]
- 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]

1.9 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]

1.10 End of Life

BIND 9.11 (Extended Support Version) will be supported until at least December, 2021. BIND 9.11-S (Supported Preview Edition) releases will continue to be published in tandem with BIND 9.11 releases until the Supported Preview Edition moves to a new branch. This may happen before BIND 9.11 reaches end of life, but not later. See https://www.isc.org/downloads/software-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/.