1 Release Notes for BIND Version 9.10.2rc2

1.1 Introduction

This document summarizes changes since the last production release of BIND on the corresponding major release branch.

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

- On servers configured to perform DNSSEC validation using managed trust anchors (i.e., keys configured explicitly via **managed-keys**, or implicitly via **dnssec-validation auto;** or **dnssec-lookaside auto;**), revoking a trust anchor and sending a new untrusted replacement could cause **named** to crash with an assertion failure. This could occur in the event of a botched key rollover, or potentially as a result of a deliberate attack if the attacker was in position to monitor the victim's DNS traffic.

  This flaw was discovered by Jan-Piet Mens, and is disclosed in CVE-2015-1349. [RT #38344]

- A flaw in delegation handling could be exploited to put **named** into an infinite loop, in which each lookup of a name server triggered additional lookups of more name servers. This has been addressed by placing limits on the number of levels of recursion **named** will allow (default 7), and on the number of queries that it will send before terminating a recursive query (default 50).

  The recursion depth limit is configured via the `max-recursion-depth` option, and the query limit via the `max-recursion-queries` option.

  The flaw was discovered by Florian Maury of ANSSI, and is disclosed in CVE-2014-8500. [RT #37580]

- Two separate problems were identified in BIND's GeoIP code that could lead to an assertion failure. One was triggered by use of both IPv4 and IPv6 address families, the other by referencing a GeoIP database in `named.conf` which was not installed. Both are covered by CVE-2014-8680. [RT #37672] [RT #37679]

  A less serious security flaw was also found in GeoIP: changes to the **geoip-directory** option in `named.conf` were ignored when running **rndc reconfig**. In theory, this could allow **named** to allow access to unintended clients.

1.4 New Features

- None

1.5 Feature Changes

- ACLs containing **geoip asnum** elements were not correctly matched unless the full organization name was specified in the ACL (as in **geoip asnum "AS1234 Example, Inc.";**). They can now match against the AS number alone (as in **geoip asnum "AS1234";**).
- When using native PKCS#11 cryptography (i.e., **configure –enable-native-pkcs11**) HSM PINs of up to 256 characters can now be used.

- NXDOMAIN responses to queries of type DS are now cached separately from those for other types. This helps when using "grafted" zones of type forward, for which the parent zone does not contain a delegation, such as local top-level domains. Previously a query of type DS for such a zone could cause the zone apex to be cached as NXDOMAIN, blocking all subsequent queries. (Note: This change is only helpful when DNSSEC validation is not enabled. "Grafted" zones without a delegation in the parent are not a recommended configuration.)
- NOTIFY messages that are sent because a zone has been updated are now given priority above NOTIFY messages that were scheduled when the server started up. This should mitigate delays in zone propagation when servers are restarted frequently.
- Errors reported when running **rndc addzone** (e.g., when a zone file cannot be loaded) have been clarified to make it easier to diagnose problems.
- Added support for OPENPGPKEY type.
- When encountering an authoritative name server whose name is an alias pointing to another name, the resolver treats this as an error and skips to the next server. Previously this happened silently; now the error will be logged to the newly-created "cname" log category.
- If named is not configured to validate the answer then allow fallback to plain DNS on timeout even when we know the server supports EDNS. This will allow the server to potentially resolve signed queries when TCP is being blocked.

1.6 Bug Fixes

- **dig**, **host** and **nslookup** aborted when encountering a name which, after appending search list elements, exceeded 255 bytes. Such names are now skipped, but processing of other names will continue. [RT #36892]
- The error message generated when **named-checkzone** or **named-checkconf -z** encounters a `$TTL` directive without a value has been clarified. [RT #37138]
- Semicolon characters (;) included in TXT records were incorrectly escaped with a backslash when the record was displayed as text. This is actually only necessary when there are no quotation marks. [RT #37159]
- When files opened for writing by **named**, such as zone journal files, were referenced more than once in `named.conf`, it could lead to file corruption as multiple threads wrote to the same file. This is now detected when loading `named.conf` and reported as an error. [RT #37172]
- **dnssec-keygen -S** failed to generate successor keys for some algorithm types (including ECDSA and GOST) due to a difference in the content of private key files. This has been corrected. [RT #37183]
- UPDATE messages that arrived too soon after an **rndc thaw** could be lost. [RT #37233]
- Forwarding of UPDATE messages did not work when they were signed with SIG(0); they resulted in a BADSIG response code. [RT #37216]
- When checking for updates to trust anchors listed in `managed-keys`, **named** now revalidates keys based on the current set of active trust anchors, without relying on any cached record of previous validation. [RT #37506]
- Large-system tuning (**configure –with-tuning=large**) caused problems on some platforms by setting a socket receive buffer size that was too large. This is now detected and corrected at run time. [RT #37187]
- When NXDOMAIN redirection is in use, queries for a name that is present in the redirection zone but a type that is not present will now return NOERROR instead of NXDOMAIN.
- When a zone contained a delegation to an IPv6 name server but not an IPv4 name server, it was possible for a memory reference to be left un-freed. This caused an assertion failure on server shutdown, but was otherwise harmless. [RT #37796]

- Due to an inadvertent removal of code in the previous release, when **named** encountered an authoritative name server which dropped all EDNS queries, it did not always try plain DNS. This has been corrected. [RT #37965]
- A regression caused nsupdate to use the default recursive servers rather than the SOA MNAME server when sending the UPDATE.
- Adjusted max-recursion-queries to accommodate the smaller initial packet sizes used in BIND 9.10 and higher when contacting authoritative servers for the first time.
- Built-in "empty" zones did not correctly inherit the "allow-transfer" ACL from the options or view. [RT #38310]
- Two leaks were fixed that could cause **named** processes to grow to very large sizes. [RT #38454]
- Fixed some bugs in RFC 5011 trust anchor management, including a memory leak and a possible loss of state information.[RT #38458]

1.7 End of Life

The end of life for BIND 9.10 is yet to be determined but will not be before BIND 9.12.0 has been released for 6 months. <https://www.isc.org/downloads/software-support-policy/>

1.8 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/>.