August 23, 2011

Contents

1 Introduction

BIND 9.8.1 is the current production release of BIND 9.8.

This document summarizes changes from BIND 9.8.0 to BIND 9.8.1. Please see the CHANGES file in the source code release for a complete list of all changes.

2 Download

The latest versions of BIND 9 software can always be found on our web site at http://www.isc.org/-downloads/all. There you will find additional information about each release, source code, and some pre-compiled versions for certain operating systems.

3 Support

Product support information is available on http://www.isc.org/services/support for paid support options. Free support is provided by our user community via a mailing list. Information on all public email lists is available at https://lists.isc.org/mailman/listinfo.

4 New Features

4.1 9.8.1

- Added a new include file with function typedefs for the DLZ "dlopen" driver. [RT #23629]
- Added a tool able to generate malformed packets to allow testing of how named handles them. [RT #24096]
- The root key is now provided in the file bind.keys allowing DNSSEC validation to be switched on at start up by adding "dnssec-validation auto;" to named.conf. If the root key provided has expired, named will log the expiration and validation will not work. More information and the most current copy of bind.keys can be found at http://www.isc.org/bind-keys. *Please note this feature was actually added in 9.8.0 but was not included in the 9.8.0 release notes. [RT #21727]

5 Security Fixes

5.1 9.8.1

- If named is configured with a response policy zone (RPZ) and a query of type RRSIG is received for a name configured for RRset replacement in that RPZ, it will trigger an INSIST and crash the server. RRSIG. [RT #24280]
- named, set up to be a caching resolver, is vulnerable to a user querying a domain with very large resource record sets (RRSets) when trying to negatively cache the response. Due to an off-by-one error, caching the response could cause named to crash. [RT #24650] [CVE-2011-1910]
- Using Response Policy Zone (RPZ) to query a wildcard CNAME label with QUERY type SIG/RRSIG, it can cause named to crash. Fix is query type independant. [RT #24715]
- Using Response Policy Zone (RPZ) with DNAME records and querying the subdomain of that label can cause named to crash. Now logs that DNAME is not supported. [RT #24766]
- Change #2912 populated the message section in replies to UPDATE requests, which some Windows clients wanted. This exposed a latent bug that allowed the response message to crash named. With this fix, change 2912 has been reduced

to copy only the zone section to the reply. A more complete fix for the latent bug will be released later. [RT #24777]

6 Feature Changes

6.1 9.8.1

- Merged in the NetBSD ATF test framework (currently version 0.12) for development of future unit tests. Use configure --with-atf to build ATF internally or configure --with-atf=prefix to use an external copy. [RT #23209]
- Added more verbose error reporting from DLZ LDAP. [RT #23402]
- The DLZ "dlopen" driver is now built by default, no longer requiring a configure option. To disable it, use "configure --without-dlopen". (Note: driver not supported on win32.) [RT #23467]
- Replaced compile time constant with STDTIME_ON_32BITS. [RT #23587]
- Make --with-gssapi default for ./configure. [RT #23738]
- Improved the startup time for an authoritative server with a large number of zones by making the zone task table of variable size rather than fixed size. This means that authoritative servers with lots of zones will be serving that zone data much sooner. [RT #24406]
- Per RFC 6303, RFC 1918 reverse zones are now part of the built-in list of empty zones. [RT #24990]

7 Bug Fixes

7.1 9.8.1

- During RFC5011 processing some journal write errors were not detected. This could lead to managed-keys changes being committed but not recorded in the journal files, causing potential inconsistencies during later processing. [RT #20256]
- A potential NULL pointer deference in the DNS64 code could cause named to terminate unexpectedly. [RT #20256]
- A state variable relating to DNSSEC could fail to be set during some infrequently-executed code paths, allowing it to be used whilst in an unitialized state during cache updates, with unpredictable results. [RT #20256]
- A potential NULL pointer deference in DNSSEC signing code could cause named to terminate unexpectedly [RT #20256]
- Several cosmetic code changes were made to silence warnings generated by a static code analysis tool. [RT #20256]

- When using the -x (sign with only KSK) option on dnssec-signzone, it could incorrectly count the number of ZSKs in the zone. (And in 9.9.0, some code cleanup and improved warning messages). [RT #20852]

- When using _builtin in named.conf, named.conf changes were not found when reloading the config file. Now checks _builtin zone arguments to see if the zone is re-usable or not. [RT #21914]

- Running dnssec-settime -f on an old-style key will now force the key to be rewritten to the new key format even if no other change has been specified, using "-P now -A now" as default values. [RT #22474]

- After an external code review, a code cleanup was done. [RT #22521]

- Cause named to terminate at startup or rndc reconfig reload to fail, if a log file specified in the conf file isn't a plain file. (RT #22771]

- named now forces the ADB cache time for glue related data to zero instead of relying on TTL. This corrects problematic behavior in cases where a server was authoritative for the A record of a nameserver for a delegated zone and was queried to recursively resolve records within that zone. [RT #22842]

- When a validating resolver got a NODATA response for DNSKEY, it was not caching the NODATA. Fixed and test added. [RT #22908]

- Fixed a bug in which zone keys that were published and but not immediately activated, automatic signing could fail to trigger. [RT #22911]

- Fixed precedence order bug with NS and DNAME records if both are present. (Also fixed timing of autosign test in 9.7+) [RT #23035]

- When a DNSSEC signed dynamic zone's signatures need to be refreshed, named would first delete the old signatures in the zone. If a private key of the same algorithm isn't available to named, the signing would fail but the old signatures would already be deleted. named now checks if it can access the private key before deleting the old signatures and leaves the old signature if no private key is found. [RT #23136]

- When using "auto-dnssec maintain" and rolling to a new key, a private-type record (only used internally by named) could be created and not marked as complete. [RT #23253]

- Fixed last autosign test report. [RT #23256]

- named didn't save gid at startup and later assumed gid 0. named now saves/restores the gid when creating creating named.pid at startup. [RT #23290]

- If the server has an IPv6 address but does not have IPv6 connectivity to the internet, dig +trace could fail attempting to use IPv6 addresses. [RT #23297]

- If named is configured with managed zones, the managed key maint timer can exercise a race condition that can crash the server. [RT #23303]
- Changing TTL did not cause dnssec-signzone to generate new signatures. [RT #23330]
- Have the validating resolver use RRSIG original TTL to compute validated RRset and RRSIG TTL. [RT #23332]
- In "make test" bin/tests/resolver, hold the socket manager lock while freeing the socket. [RT #23333]
- If named encountered a CNAME instead of a DS record when walking the chain of trust down from the trust anchor, it incorrectly stopped validating. [RT #23338]
- dns/view.h needed dns/rpz.h but it wasn't in the Makfile.in HEADERS variable. [RT #23342]
- RRSIG records could have time stamps too far in the future. [RT #23356]
- named stores cached data in an in-memory database and keeps track of how recently the data is used with a heap. The heap is stored within the cache's memory space. Under a sustained high query load and with a small cache size, this could lead to the heap exhausting the cache space. This would result in cache misses and SERVFAILs, with named never releasing the cache memory the heap used up and never recovering. This fix removes the heap into its own memory space, preventing the heap from exhausting the cache space and allowing named to recover gracefully when the high query load abates. [RT #23371]
- Fully separated key management on a per view basis. [RT #23419]
- If running on a powerpc CPU and with atomic operations enabled, named could lock up. Added sync instructions to the end of atomic operations. [RT #23469]
- If OpenSSL was built without engine support, named would have compile errors and fail to build. [RT #23473]
- If ./configure finds GOST but not elliptic curve, named fails to build. Added elliptic curve support check in GOST OpenSSL engine detection. [RT #23485]
- "rndc secroots" would abort on the first error and so could miss remaining views. [RT #23488]
- Handle isc_event_allocate failures in t_tasks test. [RT #23572]
- ixfr-from-differences {master|slave}; failed to select the master/slave zones, resulting in on diff/journal file being created. [RT #23580]
- If a DNAME substitution failed, named returned NOERROR. The correct response should be YXDOMAIN. [RT #23591]

- dns_dnssec_findzonekeys{2} used a inconsistant timestamp when determining which keys are active. This could result in some RRsets not being signed/re-signed. [RT #23642]

- Remove bin/tests/system/logfileconfig/ns1/named.conf and add setup.sh in order to resolve changing named.conf issue. [RT #23687]

- NOTIFY messages were not being sent when generating a NSEC3 chain incrementally. [RT #23702]

- DDNS updates using SIG(0) with update-policy match type "external" could cause a crash. Also fixed nsupdate core dump on shutdown when using a SIG(0) key, due to the key not being freed. [RT #23735]

- Zones using automatic key maintenance could fail to check the key repository for updates. named now checks once per hour and the automatic check bug has been fixed. [RT #23744]

- named now uses the correct strtok/strtok_r/strtok_s based on OS. [RT #23747]

- Signatures for records at the zone apex could go stale due to an incorrect timer setting. [RT #23769]

- The autosign tests attempted to open ports within reserved ranges. Test now avoids those ports. [RT #23957]

- GSS TGIS test was failing, since log_cred() caused KRB5_KTNAME to be cached. Now sets KRB5_KTNAME before calling log_cred() in dst_gssapi_acceptctx(). [RT #24004]

- named, acting as authoritative server for DLZ zones, was not correctly setting the authoritative (AA) bit. [RT #24146]

- Clean up some cross-compiling issues and added two undocumented configure options, --with-gost and --with-rlimtype, to allow over-riding default settings (gost=no and rlimtype="long int") when cross-compiling. [RT #24367]

- When trying sign with NSEC3, if dnssec-signzone couldn't find the KSK, it would give an incorrect error "NSEC3 iterations too big for weakest DNSKEY strength" rather than the correct "failed to find keys at the zone apex: not found" [RT #24369]

- Configuring 'dnssec-validation auto' in a view instead of in the options statement could trigger an assertion failure in named-checkconf. [RT #24382]

- Improved consistency checks for dnssec-enable and dnssec-validation, added test cases to the checkconf system test. [RT #24398]

- If named is configured to be both authoritative and recursive and receives a recursive query for a CNAME in a zone that it is authoritative for, if that CNAME also points to a zone the server is authoritative for, the recursive part of name will not follow the CNAME change and the response will not be a complete CNAME chain. [RT #24455]
- nsupdate could dump core on shutdown when using SIG(0) keys. [RT #24604]
- Named could fail to validate zones list in a DLV that validated insecure without using DLV and had DS records in the parent zone. [RT #24631]
- dnssec-signzone now records timestamps just before and just after signing, improving the accuracy of signing statistics. [RT #16030]
- If allow-new-zones was set to yes and name-based ACLs were used, named could crash when "rndc reconfig" was issued. [RT #22739]
- RT #23136 fixed a problem where named would delete old signatures even when the private key wasn't available to re-sign the zone, resulting in a zone with missing signatures. This fix (CHANGES 3114) did not completely fix all issues. [RT #24577]
- A bug in FreeBSD kernels causes IPv6 UDP responses greater than 1280 bytes to not fragment as they should. Until there is a kernel fix, named will work around this by setting IPV6_USE_MIN_MTU on a per packet basis. [RT #24950]

8 Known issues in this release

- None.

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/supportisc.