BIND 9.10.6-P1 Release Notes

Author: **Michael McNally** Reference Number: **AA-01548** Views: **2029** Created: **2018-01-16 20:26**
Last Updated: **2018-01-16 20:26**

Introduction

This document summarizes changes since BIND 9.10.6.

BIND 9.10.6-P1 addresses the security issue described in CVE-2017-3145.

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.

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 .

Windows XP No Longer Supported

As of BIND 9.10.6, Windows XP is no longer a supported platform for BIND, and Windows XP binaries are no longer available for download from ISC.

Security Fixes

- 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. (The delay will be addressed in an upcoming maintenance release.) This bug is disclosed in CVE-2017-3145. [RT #46839]

- 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]

Feature Changes

- **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]

Bug Fixes

- 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]

- 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]

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/

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/.

For assistance with problems and questions for which you have not been able to find an answer in our Knowledge Base, we recommend searching our community mailing list archives and/or posting your question there (you will need to register there first for your posts to be accepted). The bind-users and the dhcp-users lists particularly have a long-standing and active membership.

ISC relies on the financial support of the community to fund the development of its open source software products. If you would like to support future product evolution and maintenance as well having peace of mind knowing that our team of experts are poised to provide you with individual technical assistance whenever you call upon them, then please consider our Professional Subscription Support services - details can be found on our main website.