Open Source For an Open Internet

ISC Subscriber News

2026 Q1

Important updates for ISC's BIND 9, Kea DHCP, Stork, and ISC DHCP support subscribers.

DNS News

BIND Update

BIND Development and LLMs

The BIND team is, like most software engineering teams, experimenting to look for ways that LLMs might help us with development tasks. We are always interested in useful tools and automation. So far, we have found some successes ranging from reviewing or even suggesting commit messages, refactoring test cases (where it was far less efficient than our QA engineer), and running other experiments. However, overall, we are still extremely mistrustful of LLM-authored code, due to many experiences in which AIs reported bugs in code that doesn't exist, or wrote tests that would pass even without the proposed fixes, or otherwise provided unusable results. The overall impact of AI on the BIND team, so far, is an increase in "slop" vulnerability reports, which may be very detailed and sound very plausible, but often do not actually turn out to be real code or cause real problems.

Therefore, we want to reassure our support customers that, at ISC, the humans remain firmly in control. We will continue to assess the use of AI to maintain awareness of developments in this field and potential impact on our products. We have also added a section on the use of AI tools to the BIND contribution guidelines.

Other updates

- In January we published a 2025 BIND 9 Development Report. We encourage you to read it for an overview of what we accomplished last year.
- We recently posted a blog on recursive performance, comparing 9.20 to 9.18. The TL;dr is that performance is very similar; the start-up cold-cache performance for a very busy resolver is better with 9.20, and in low-traffic scenarios BIND 9.20 can consume more memory than 9.18, but as traffic increases, BIND 9.20 uses less memory than BIND 9.18.
- Although ISC does not offer bug bounties, we accepted an offer from the European Commission to fund a limited-time bug bounty for BIND 9, managed by YesWeHack. The program launched at the end of November 2025 and has generated a total of 130 reports so far. The first ones were nearly all dismissed as junk, but we are getting some actionable reports now.

Looking forward to BIND 9.22

The next stable version of BIND, 9.22, is scheduled for Q2 2026. It will likely not be ready until the very end of the quarter. When we release 9.22, we will also end maintenance for BIND 9.18. Here is some of the work in process that we hope to include in 9.22.

- One of the most consequential changes in 9.22 is a shift towards a parent-centric resolver.

  The `named` resolver will use a separate "delegation database" to store zone referral data instead of the DNS cache. This new database holds the NS RRset on the parent side of a zone cut, as well as necessary glue records that were included in the referral. The NS RRset from the child side is cached in the DNS cache and is not used for name resolution.

  This will be a step toward simplifying resolver logic and also supporting DELEG referrals.
- We also expect to have our initial support for the new DELEG protocol. Deleg is the biggest change in the DNS in a decade. We hope it will put more control in the hands of the operators, significantly simplify provisioning of zone parameters, and improve security.
- Matthijs Mekking gave a talk at the recent ICANN DNSSEC workshop on Generalized Notifications in BIND 9.22. This new notify use case nudges the parent to update a DS record.
- Already discussed in a previous newsletter, the ability to show the effective running configuration was added in response to popular request. (`rndc showconf -effective`)
- As announced via a support email, we plan to integrate the ECS and Cisco Umbrella features into the open source, and retire the -S edition branch with 9.20-S.
- And finally, zone templates, implemented early in the 9.21 cycle, will simplify the configuration of multiple similar zones.

Kea/DHCP News

The Kea security audit is now public. As described in our blog, although the audit did not find any significant software vulnerabilities, it did help us establish an ongoing fuzz-testing program, and gave us a headstart on producing software BOMs (bills of materials).

We have recently posted the results of our performance testing for Kea 3.0.2.

The team is hard at work maintaining and developing Kea. Kea 3.2, planned for May or June, will complete the process of removing the Control Agent, and address a number of issues with socket and interface handling. We are updating the Free Leases Queue (FLQ) allocator to work on shared MySQL, MariaDB, and PostgreSQL databases, an option we added for users wanting two Kea servers to share a single lease database backend (see the KB article on issues with sharing a lease DB). We also seeing more requests for documentation and extensions to our hub-and-spoke failover support, some of which may make it into Kea 3.2.

With the release of Kea 3.2, maintenance of Kea 2.6 will end. Kea 3.0 is designated as a long-term support version, so that will be supported until mid-2028.

New and updated KB articles from our support team:

- Kea API and Control Sockets
- Ports Used by Kea
- Kea: Use Unique Databases
- Using Kea Config File Includes
- Things to be aware of when upgrading to Kea 3.0 (updated)
- How to use the perfdhcp testing tool (updated)
- Stork 2.4 and Kea socket permissions

Stork News

The Stork security audit performed for us by 7A Security is now public. The audit found several issues we wanted to fix, so we delayed publication until those were resolved. They were all addressed with Stork 2.4, except for the recommendation that we add support for multi-factor authentication, which is in progress now and will hopefully be finished before the release of 2.6.

Stork 2.4 now supports Kea direct API mode, table sorting, and several features for DNS authoritative users. Our blog on the release of Stork 2.4 includes a number of screenshots, which are a good way of quickly seeing what is new. For example, the screenshot below shows a listing of all the records in a particular zone. Other views show which servers are serving a specific zone, with what zone serial number, and when the zone was last updated.

We also posted a walkthrough of the new DNS features on YouTube.

With the release of Stork 2.4, Stork 2.2 is now end-of-life, per our published release plan.

Work in Process
A few of the most exciting features we are working on currently include:

- Adding support for collecting and searching lease activity to support many troubleshooting use cases. The challenge is to do this at scale, without hampering the Kea servers' primary activity.
- Adding support for federated authentication, using OpenID Connect. We hope this will also address the requirement for multi-factor authentication.
- Adding a configuration file for Stork agent. This requirement is driven by increasing configuration complexity, some of which is due to our new support for DNS.
- Monitoring DNS zone transfers. Stork is ideally positioned, with a view of both the primary and secondary servers, to monitor the web of zone transfers.
- Adding Stork support for the Kea Configuration Backend. Currently Stork reads and modifies the Kea configuration stored on the Kea server only. Adapting it to work with the model where the configuration is stored in a database, and shared across multiple Kea servers, is a major change.

If you have thoughts about any of the design documents linked above, feel free to raise them with us in a support ticket. We would love your feedback. These features are significant efforts that will take multiple releases to complete, so even though they are already in process, there is still time to consider more input.

Meet an ISC Staff Member!
Let us introduce you to our Director of Sales, T. Marc Jones!

Your Support Subscription

Why are we seeing so many CVEs from ISC now?

The rapid evolution of AI-assisted tools for software analysis is fueling an explosion in vulnerability reports. This is a general observation across all of open source, and ISC is also seeing a sharp increase. In addition, ISC accepted a generous offer from the European Commission to sponsor a bug bounty for BIND, through the YesWeHack program. The bug bounty hunters on that platform are also contributing to a windfall of new security findings. Although no one is happy to be issuing CVEs, we are grateful to the reporters who allow us to improve the stability of our software. It is important to stay on top of this trend, because the bad actors certainly will be.

Upcoming Holiday Schedule for ISC Support

ISC's support department will be closed for regular business on:

- April 3 (Good Friday)
- May 25 (US Memorial Day)
- June 19 (US Juneteenth)

Normal-priority tickets opened on those days will be responded to on the first business day following our return.

Critical-priority tickets will, as always, be responded to based on your organization's critical-ticket SLA. Please check our support portal and/or contact your account manager if you have questions about your level of support from ISC.

Hope to see you soon!

ISC staff would love to meet you at any of these upcoming events:
OARC45: Edinburgh, Scotland, May 16-17
RIPE92: Edinburgh, Scotland, May 18-22
NANOG 97: Bellevue, Washington, June 1-3
BSDCan 2026: Ottawa, Ontario, June 17-20

ISC staff members often give presentations at industry meetings and conferences. Presentation slides and recording links (when available) are posted at https://www.isc.org/presentations/.

ISC is on Bluesky (https://bsky.app/profile/isc.org) and Mastodon (https://fosstodon.org/@iscdotorg)! Please follow us for timely news and updates.