

Internet Systems Consortium, Inc.

2021 Annual Report

Email: info@isc.org
Website: isc.org
Telephone: +1 650 423 1300



INTERNET SYSTEMS CONSORTIUM, INC. ANNUAL REPORT 2021

© 2022 INTERNET SYSTEMS CONSORTIUM, INC.

Internet Systems Consortium refers to Internet Systems Consortium, Inc. (a not-for-profit company) and its wholly owned subsidiary Internet Systems Corporation, both incorporated in Delaware with headquarters in New Hampshire, USA.

MAIN OFFICE:

60 EXETER ROAD, SUITE 104
NEWMARKET, NEW HAMPSHIRE 03857 USA

MAILING ADDRESS:

PO BOX 360
NEWMARKET, NEW HAMPSHIRE 03857 USA

+1 650 423 1300
ISC.ORG
INFO@ISC.ORG

All trademarks referenced or mentioned in this report are the property of their respective owners.

TABLE OF CONTENTS

LETTER FROM THE PRESIDENT	1	KEA DHCP, ISC DHCP, AND STORK SOFTWARE	10
WHO WE ARE	2	Growing User Base	10
		HA+MT and Performance	10
2021 HIGHLIGHTS	3	GSS-TSIG	10
F-Root Operations and RSO Governance	3	Security	10
Public Policy	3	Quality Assurance	10
2022 Goals	4	ISC DHCP	11
Our Thanks	4	Stork	11
2021 FINANCIAL OVERVIEW	5	SOFTWARE SUPPORT	12
Revenues	5	F-ROOT AND TECHNICAL OPERATIONS	14
Expenses	6	New Sites	14
		Upgraded Sites	14
2021 CONSOLIDATED FINANCIAL INFORMATION	7	THE PEOPLE OF ISC	15
BIND 9 DNS SOFTWARE	8	Board of Directors	15
Release Schedule	8	Management	15
BIND 9.16	8	Professional Affiliations	15
Performance	8	Contributions to Other Projects	15
Memory Usage	8	Public Webinars and Presentations	16
DNS Privacy	8	Other Activities of Note	16
Protocol Engineering	8	OUR CONTRIBUTORS	17
Documentation	9		
Security	9		
Performance Impacts From Zone Transfers	9		
PKCS#11	9		
Build System	9		
Windows Support	9		
Quality Assurance	9		
Future Development	9		

LETTER FROM THE PRESIDENT

As we reach the beginning of the third year of the Covid-19 pandemic, it's difficult not to be disappointed. A year ago, we were looking at the wide-scale rollout of vaccines that promised to get everything back to normal, but instead, most of us are still in limbo. But rather than feel depressed, we are cautiously optimistic about the future.

Our financial results have been very good. Revenues have been on an uptick, reaching over \$7 million in 2021, and almost none of our paying customers have chosen to stop supporting us. We have been cautious in hiring and have managed to put aside a reasonable cash reserve, so all things considered, at least we are not worried about money for the moment.



As an open source Internet software company, we're big believers in the value of free and open communications for all. As the Internet has become more and more essential for everyday contact around the globe, we remain committed to keeping our software freely accessible to all. We feel strongly that centralizing control of the Internet in the hands of a few huge players would do a huge disservice to millions of individuals and organizations worldwide, and we are proud to do our part to keep the Internet open and available to everyone.

Of course, we are still a business: our staff members need to support their families, and we have bills to pay. But we do not believe that a relentless pursuit of profits benefits our stakeholders or our society.

We think we've found a sweet spot: the support contracts we sell to organizations and companies around the world offer them security and stability, and they enable us to continue developing the software that anyone can download. Our customers know that we are here to help keep their DNS and DHCP services running smoothly, while other users benefit from widely available software with community support.

Incredibly, we are approaching the 40th anniversary of the initial development of BIND, and it is difficult to overstate the significance of DNS and DHCP in our daily lives - even though the vast majority of people don't know what those letters even stand for (Domain Name System and Dynamic Host Configuration Protocol, in case you're one of them). These two protocols touch nearly every aspect of modern society, and their importance is likely to continue for quite a while. ISC will keep pursuing our mission of developing software and offering services in support of the Internet infrastructure well into the future.

Regards,

Jeff Osborn

WHO WE ARE

ISC develops and maintains four open source Internet networking software packages: [BIND 9](#), [ISC DHCP](#), and [Kea DHCP](#), as well as our new Kea monitoring program, Stork. BIND 9, ISC's Domain Name System (DNS) software program, is widely used on the Internet by enterprises and service providers, offering a robust and stable platform on top of which organizations can build distributed computing systems. ISC DHCP is our classic implementation of the Dynamic Host Configuration Protocol for connection to an IP network, offering a complete solution for implementing DHCP servers, relay agents, and clients. ISC DHCP is a mature program with many features, but the software is cumbersome to maintain and update. Kea DHCP, in conjunction with the Stork management platform, is ISC's intended replacement for ISC DHCP. Kea offers a modular design with database management for easy dynamic reconfiguration, while Stork provides a web-based graphical dashboard.

ISC's staff contribute to various Internet governance and community initiatives, and ISC engineers have written or co-authored more than 100 of the [technical standards \(RFCs\)](#) that are essential to interoperability on the Internet.

Since the company's founding in 1994, ISC's staff members have pursued the goal of "open source for an open Internet." That pursuit continues today.

ISC's open source software offers commercial-grade, rigorously vetted code with professional support for our customers' mission-critical Internet infrastructure. Our business model of paid subscriptions for open source works well for us. It aligns our incentives appropriately as we work for the success of our stakeholders: our subscription customers, and by extension all users.

ISC is proud of its multinational staff. In 2021, the total number of native languages spoken at ISC was thirteen (English [American, British, AND Australian], Polish, Czech, French, Romanian, Welsh, German, Dutch, Ukrainian, Russian, and Armenian).



A scene from one of our many, many Zoom meetings in 2021. We know you get it.

2021 HIGHLIGHTS

2021 was a busy year for ISC. We (and everyone else) mostly stayed home to try to keep ourselves and our families safe, but that didn't mean we weren't working. We put out monthly releases of BIND 9 (including the new stable branch, 9.18), as well as 11 Kea DHCP releases (including 2.0.0) and nine Stork releases (including 1.0).

Although our transition to BIND 9.16 as an extended-support version did not go as smoothly as we'd hoped due to some refactoring issues, we successfully completed those in 2021; the new stable branch, BIND 9.18, was released in the first weeks of 2022, and so far it is solid and working well. The Kea user base is growing and both Kea and Stork are maturing. We continue to balance long-term ambitious changes with smaller bug fixes and new features. A significant focus for us this year was improvement of our quality-assurance processes for all our software.

We made continued progress in updating and adding F-Root nodes. We also increased participation and leadership from ISC in policy discussions about Root Server Operator (RSO) governance, with the active engagement of ISC's general counsel, Rob Carolina.

It is always reassuring to see that ISC can still attract talented people who are excited to work on open source. We added new staff on the BIND and DHCP development teams, and both new management and staff for our support team.

Public Policy

The European Union Proposal for a new [NIS2 Directive](#) became a significant focus for ISC in March 2021. NIS2 (a proposed law building on the original NIS Directive to strengthen European approaches to cybersecurity) was drafted in a manner that appeared to call for EU member states to regulate the cybersecurity arrangements of all 12 global RSOs.

While ISC applauds the desire to strengthen cyberdefenses, [ISC submitted public comments](#) on the proposed Directive specifically calling out the danger of any sovereign state attempting to directly regulate the world's root server system (RSS). We pointed out that, far from enhancing the resilience and security of the Internet, sovereign intervention in RSS operations could destabilize the RSS and DNS. We explained that regulatory intervention in the RSS by one sovereign state could prompt (potentially conflicting) regulatory intervention by other sovereign states. We and some of our fellow RSOs suggested that this would, in turn, risk fragmenting the Internet as we know it.

The European Parliament subsequently amended the draft Directive in late 2021 to take root servers out of its scope, but the matter is not finally resolved. We are waiting to see whether the European Council will attempt to negotiate the reintroduction of the RSS into the law, and this issue will remain important to us in 2022.

Although worldwide economies continue to see significant turmoil, ISC's financial picture is very solid. We ended 2021 with nearly 150 support subscribers - over 90% of them renewals from 2020 - with new customers more than making up for the few we lost. More of our customers are subscribing for both BIND and Kea support, and we are gaining more traction with larger enterprises. However, we know that recessions are inevitable, and do our best to keep our expenses manageable.

F-Root Operations and RSO Governance

ISC's status as a root service operator (RSO) spawned some significant work related to the ongoing discussions of a new root server system governance structure (RSS GS). In mid-2021, the community of 12 RSOs began to review and discuss a draft proposal for a new RSS GS put forward by the Root Server System Governance Working Group (RSS GWG), chartered by ICANN.

This resulted in the adoption and publication on 17 November 2021 of "RSSAC058: Success Criteria for RSS Governance Structure" and "RSSAC059: RSSAC Advisory on Success Criteria for the Root Server System Governance Structure." These documents were warmly received by the ICANN Board of Directors and they will now form part of a revised RSS GWG work plan.

2022 Goals

We look forward to another successful year in 2022 and hope that it will bring peace, prosperity, and good health to all of our customers, users, and staff members.

We plan to continue fixing BIND 9 bugs, adding new features requested by customers and users, and refactoring old code. A major project planned for the next development cycle is the refactoring of the venerable red-black tree database (RBTDB) implementation, used to store authoritative zone records and cached RRsets. We expect to add a developer and a quality assurance engineer to the BIND team this year.

On the Kea DHCP front, our key initiatives are to continue improving secured administrative access to Kea with Transport Layer Security (TLS); to add some role-based access controls; and to focus on new customer requests as Kea meets growing operational requirements. We are also planning to expand Stork to provide support for Kea configuration changes.

We also expect to release ISC DHCP 4.4.3, which will be the last release with both the client and relay components.

We are closely watching the development of new standards and requirements for software security as a result of the 2021 [US Executive Order on Cybersecurity](#) and are working to ensure all our software products are compliant. We recognize the importance of software supply chain security and are committed to keeping our customers' deployments as safe as possible.

Our support team anticipates another busy year helping our customers maintain their DNS and DHCP operations. We will be migrating to a new support ticketing system (Salesforce), which should offer some new features to our customers and make their experience with us even better. In conjunction with the new ticketing system, we plan to perform a review of our support processes, specifically the Advance Security Notification, software delivery, and customer/account maintenance processes. Finally, we hope to improve our knowledge management, specifically via better maintenance of ISC's [Knowledgebase](#) and software administrators' manuals.

Our Thanks

Our greatest thanks go to the loyal open source users who continue to support ISC, many of whom have been paid customers of ours for more than a decade. These include some of the most capable independent operators and enterprises in the world.

We also owe a debt to all the wonderful open source users who have submitted feedback and patches, and the open source packagers who maintain distributions for our users. We regard many of these collaborators as our friends.

In 2021 we received generous unrestricted donations from the craigslist Charitable Fund (CCF), Verisign, Deteque, and Jisc.

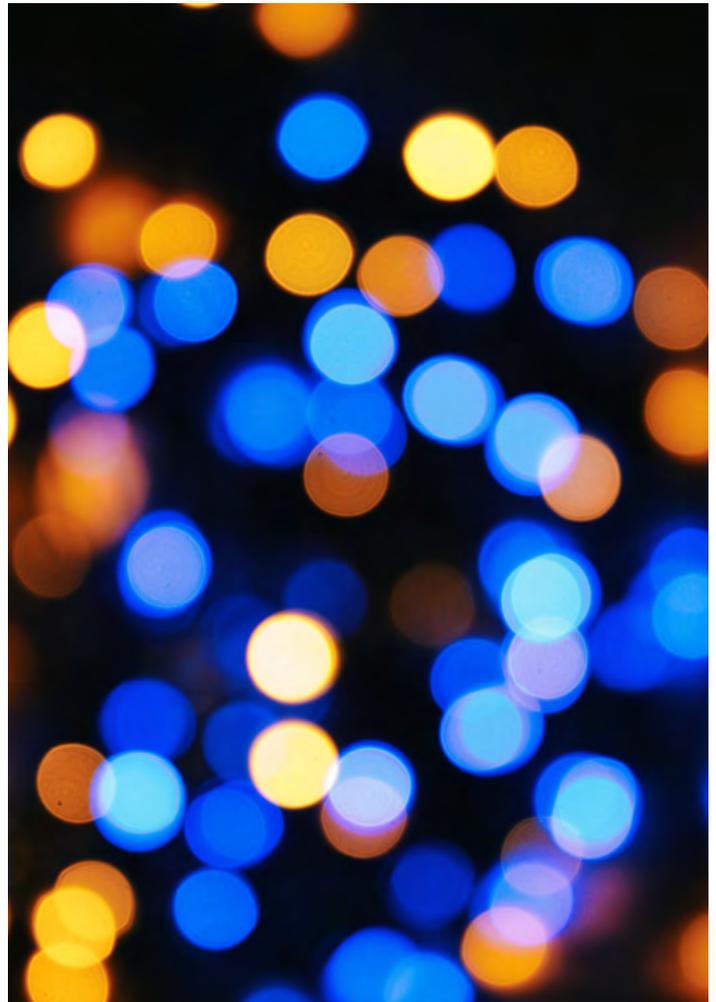


Photo by [Alinenok](#) on [Unsplash](#)

2021 FINANCIAL OVERVIEW

Revenues

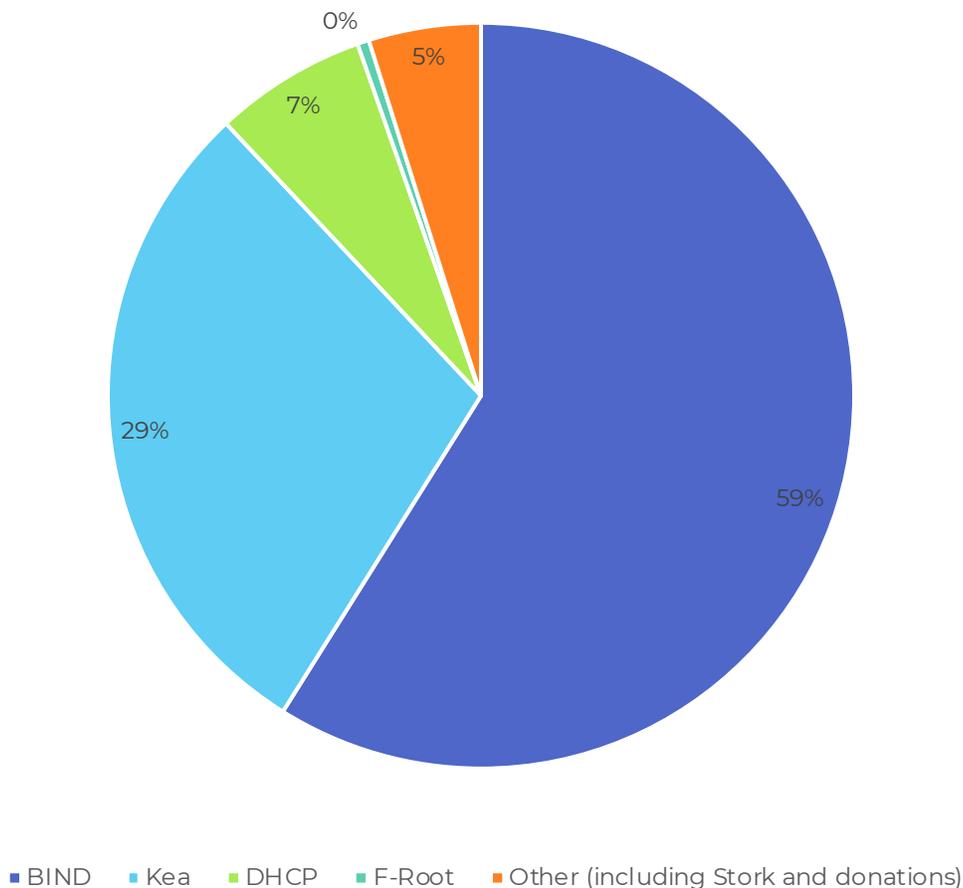
ISC's open source software is available for free download; we fund our operations with paid support contracts for our software, which also include special software features. In 2021, 59% of our revenues came from our flagship product, BIND 9. Another 36% came from our DHCP offerings, ISC DHCP and Kea DHCP. Since its introduction in 2017, Kea has become an important revenue source for ISC and we expect its significance to continue growing.

The remaining 5% of the company's 2021 revenues came from F-Root and donations.

We gained 17 new support contracts in 2021, and lost only six.

Although normally our staff team is relatively static, 2021 was a significant hiring year for ISC: we had eight new engineers join our ranks during the year. Of those, four are additions to our support team, two are BIND engineers, and two work on Kea.

2021 Revenues by Service

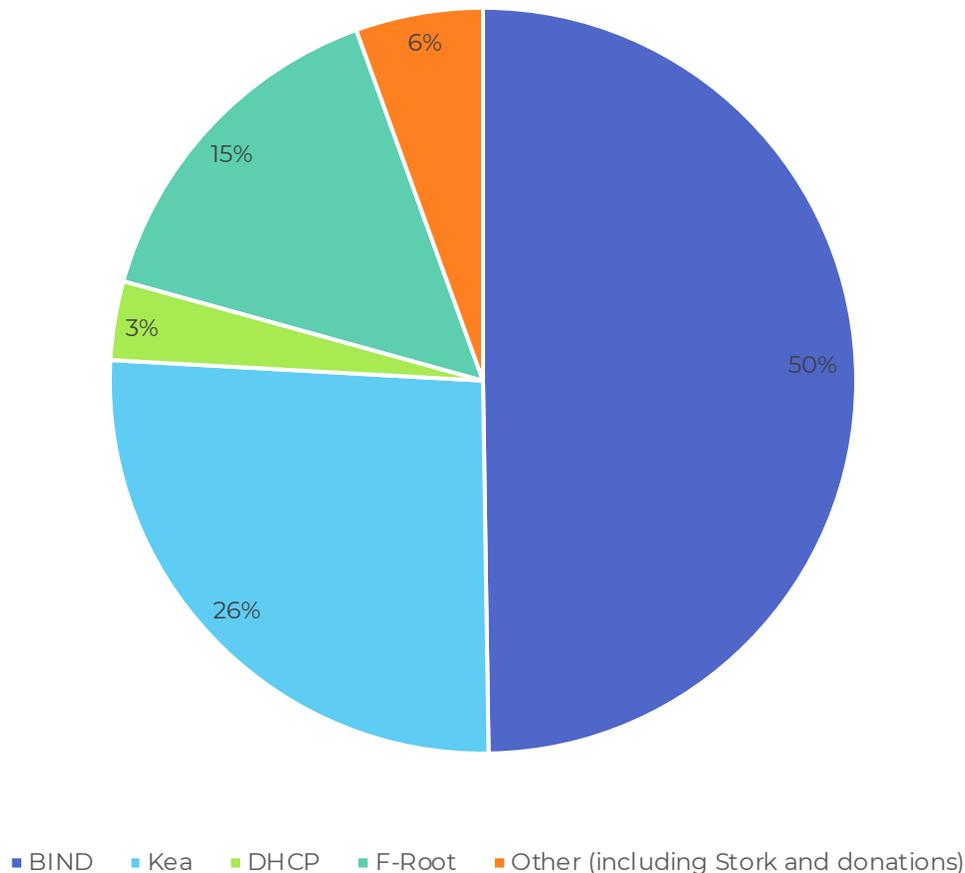


Expenses

ISC's staff are leaders in the Internet industry and represent the majority of the company's costs. Other than personnel, ISC's expenses include bandwidth, network and equipment depreciation, travel (although there was almost none of that in 2021), taxes, utilities, and maintenance – and very little else. We are proud of the efficiency and cost-effectiveness of our operations.

At the end of 2021, we had 37 staff members in 12 countries (the US, the UK, France, Austria, Denmark, Poland, Romania, Czechia, Australia, the Netherlands, Ukraine, and Armenia). Eighteen people worked in Software Engineering and Quality Assurance; six in Support; five in Sales and Marketing; four in Finance and Executive Operations; and four in F-Root and Technical Operations.

2021 Expenses by Service



2021 CONSOLIDATED FINANCIAL INFORMATION

	2021	2021	2021	2021	2021
<i>Numbers in thousands of dollars</i>	Q1	Q2	Q3	Q4	Total
Actual					
Revenue	1,502	1,929	1,906	1,779	7,116
Expense	1,427	1,425	1,360	2,078	6,291
Net Income	74	504	546	(299)	825
Budget					
Revenue	1,374	1,431	1,347	1,507	5,659
Expense*	1,347	1,347	1,382	1,581	5,657
Net Income	27	84	(35)	(74)	2
Delta of Actuals to Budget					
Revenue	128	498	559	272	1,457
Expense	80	78	(22)	497	634
Net Income	47	420	581	(225)	823

* Excludes depreciation expense

	2021	2021	2021	2021
	Q1	Q2	Q3	Q4
Headcount**				
Forecast/Budget	36	36	36	36
Actual	35	34	36	36

** At end of quarter



BIND 9 DNS SOFTWARE

Even with the pandemic raging, 2021 was a productive year for the BIND 9 team. Notably, we stabilized BIND 9.16 to a point that it has been designated as an Extended Support Version (ESV).

At the beginning of 2021, Petr Špaček joined the BIND 9 team and began improving our recursive performance testing. Later in the year, Aram Sargsyan jumped into the fray, working on OpenSSL improvements. In another major achievement, Mark Andrews hit 20 years at the company; he was named Distinguished Engineer to reflect his long-time commitment to BIND 9.

Release Schedule

At the beginning of 2021, we decided to [modify our BIND release model](#) again, to lengthen the time between major branches and provide extended support for every stable branch. This leaves us with a four-year support cycle for each Stable/ESV release and a two-year overlap to allow a graceful migration period for our users.

We have reduced the changes backported to the BIND 9.11 branch to a bare minimum, keeping the promise that only security and high-impact issues will be fixed in BIND 9.11 as it nears end-of-life. Code changes in BIND 9.16 were unfortunately greater in the first half of 2021, but since we marked BIND 9.16 as ESV in mid-year, we are gradually reducing the amount of work backported from the development branch to BIND 9.16.

BIND 9.16

The BIND 9.16 network manager code was stabilized in the first half of 2021 to the point where it is stable and reliable. The TCP-handling parts of the network manager code had to be rewritten from scratch, but while this was a difficult choice to make during a stable cycle, it has proved to be reliable since that code was merged.

Performance

BIND 9.16 authoritative performance was already in the “good enough” ballpark, achieving around 1Mqps (millions of queries per second); during the year, we significantly improved the recursive performance testing, building on Petr’s experience. The new recursive testing framework allowed us to identify and fix bottlenecks in the existing code, which reduced the number of threads by

one-third by moving internal tasks to run in the network manager worker loops. This at least doubles BIND 9.16’s performance compared to BIND 9.11; we published this [blog post](#) where recursive performance is discussed in more detail. We continued to work in this area, refactoring the dispatch (DNS client) code in the BIND 9.18 release, bringing even higher performance to the recursive function of BIND 9 while reducing memory consumption at the same time.

Memory Usage

In BIND 9.18, the BIND 9 native memory allocator was removed and replaced by jemalloc, which could be optionally compiled in and is recommended for all workloads. BIND 9.18 uses the same or less memory than BIND 9.11 while the performance has more than doubled.

Users upgrading from 9.11 to 9.16 reported significantly higher memory usage. We fixed this by backporting some of the improvements made for 9.18 to 9.16. This is discussed in length in a [Knowledgebase \(KB\) article](#).

DNS Privacy

The new BIND 9.18 includes support for DoT (DNS over TLS), XoT (XFR over TLS), and DoH (DNS over HTTPS), protocols that add encryption-layer support for the new privacy-focused protocols. This is important for users who want to enhance the privacy of their client-resolver connections without relying on the “big tech” providers. We will continue our work in this area, so BIND 9 will keep being a great choice for people who want additional privacy.

Protocol Engineering

ISC’s engineers participate in IETF protocol development. We have collaborated with NLNetLabs on interoperability changes to DNS Cookies - both writing an RFC standard and implementing the new SipHash-based algorithm for DNS Cookies. We continue to collaborate on the new iteration of Catalog Zones that should make all the open source versions interoperable, allowing for more diversity in secondary servers. BIND 9 now includes support for HTTPSRRV records, finally solving the long-standing “CNAME-flattening/ANAME” problem.

Documentation

The BIND Administrative Reference Manual (ARM) has been converted from DocBook (XML-based) to Sphinx (RST-based) and is now regularly published at <https://bind9.readthedocs.io/>.

Security

In 2021, BIND 9.11 announced four CVEs (security vulnerabilities) and BIND 9.16 announced five. Details can be found in the [BIND 9 Security Vulnerability Matrix](#) in our Knowledgebase.

During investigation of a GSS-TSIG vulnerability in the BIND 9 implementation of SPNEGO, BIND 9 engineers found (and responsibly disclosed, of course) a serious vulnerability of the Heimdal Kerberos implementation used in FreeBSD and other BSDs.

Performance Impacts From Zone Transfers

After at least one customer reported performance degradation during zone transfers when deploying BIND 9.16, we analyzed the code and implemented a new approach to these transfers. Previously, BIND 9 used a technique where it would “quantize” long-running jobs into smaller chunks and intermingle this small-chunk processing into regular query-response processing. Under the new approach, long-running jobs are offloaded to a separate thread pool that runs the jobs independently, leaving scheduling to the operating-system kernel. Instead of quantizing the job into arbitrarily sized chunks, the long-running job blocks the other threads for the least possible time - locking and unlocking the shared resources for only a short period.

PKCS#11

During the development cycle, it became clear that supporting different implementations of PKCS#11 natively in BIND was inefficient and expensive. As part

of our commitment to open source, we contributed to improving the libp11-based engine_pkcs11 for OpenSSL. Performance and stability were improved to the point where we were able to drop BIND’s native PKCS#11 implementation in favor of the OpenSSL-based PKCS#11 implemented in engine_pkcs11. In 2022, we plan to implement the PKCS#11 engine for OpenSSL 1.x and the PKCS#11 driver for OpenSSL 3.x, without using libp11.

Build System

The build system used by BIND 9 has been completely rewritten to use autoconf, automake, and libtool, making it more modern and easier to understand and modify.

Windows Support

Support for building BIND 9 on Windows has been removed in the development release; the last major release supporting Windows is 9.16.

Quality Assurance

The [BIND 9 QA team](#) implemented a unified monthly release cycle for both security and normal patch releases, bringing more predictability and stability to the release process.

Continuous Integration (CI) now runs completely in GitLab, and we no longer use Jenkins nor the even older “Robie.” All their functions were either moved to the GitLab CI or the need for them has been eliminated.

The QA team designed and implemented a completely new recursive performance testing framework which provides much-needed data on which to base decisions. This new framework nicely complements our existing authoritative performance testing in ISC’s [perflab](#).

KEA DHCP, ISC DHCP, AND STORK SOFTWARE

Despite all the craziness in the world and in the personal lives of some team members, 2021 was a very good year for the Kea DHCP project. We released Kea 2.0.0, which was a major milestone in the project history. Bumping the major number to 2 (1.0 was first released in 2015) reflects the overall feeling that the code base has matured significantly and is usable even in the largest and most demanding ISP deployments.

Growing User Base

Our confidence in Kea is backed up by the growing number of users. We ended 2021 with nearly 50 Kea support customers - a substantial increase from 32 at the end of 2020. During the year we closed 521 GitLab engineering tickets, including new features, bug fixes, documentation improvements, and more. We shipped 12 releases, several code drops, and quite a few patches to customers who couldn't wait for the next monthly release. We also saw more support customers who are not ISPs; the expansion into enterprise and university markets is both exciting and challenging. The trend is also visible in the new features being requested and implemented.

HA+MT and Performance

Kea is now fully multi-threaded (MT), including the tricky High Availability (HA) scenario with two servers communicating over multiple connections and multiple threads. Being able to process lease updates in parallel (with the bottlenecks of a shared single UNIX socket and single TCP connection eliminated) delivered impressive results. In the most extreme scenarios, Kea performance improved tenfold over prior versions. More typical scenarios are less dramatic, but Kea 2.0 is still several times more performant than Kea 1.8. In the most efficient scenario, Kea is able to assign 38,000 new leases per second; we're approaching levels where our testing tools are not able to keep up. It's a good problem to have.

GSS-TSIG

We completed a major sponsored development project: GSS-TSIG. This was by far the biggest custom feature in the history of Kea. GSS-TSIG provides integration with Microsoft Windows environments, using Active Directory which in turn uses Kerberos. The team worked closely with

the sponsoring customer and provided many engineering checkpoints, so the customer could oversee the technical details and perform early integration.

Security

For much of its early life Kea was focused on delivering protocol features, but since it is more or less complete in this regard, our development efforts have now shifted towards improving its management. This is of vital interest for many existing and prospective users. Kea's RESTful API interface can now be protected with Transport Layer Security (TLS), including the mutual mode where both server and connecting client certificates are validated. We also developed support for MySQL connections over TLS, and added a section to the Kea Administrator Reference Manual (ARM) about security.

2021 was the second year in a row when we did not publish any security advisories for Kea. However, our internal "[peanut gallery](#)" fears that due to the new TLS and Kerberos code in Kea, our good fortune with security incidents may come to an end. Time will tell!

Quality Assurance

We migrated our automated Kea build and testing farm to Amazon Web Services (AWS), and took this opportunity to review and significantly update our testing procedures. Previously, we had a fixed number of virtual machines (VMs) that were always on. With AWS, we migrated to an on-demand mode, where the VMs are created to run a specific set of tests and then are destroyed afterward. This allows us to run tests on more systems. At the end of the year, we had 3,789 system tests, running on 14 operating systems (various versions of Alpine, CentOS, Debian, Fedora, FreeBSD, and Ubuntu). With over 8,400 unit-tests in Kea code, that gives us over 118,000 test/OS combinations that are run on every commit to the master branch.

As of the end of 2021, the Kea sources consisted of 1,008,159 lines of code. That code is now scrutinized using multiple automated tools, including but not limited to Coverity Scan, TSAN (thread sanitizer), ASAN (address sanitizer), UBSAN (Undefined Behavior Sanitizer), gcov (coverage report), and more. We also run extensive

performance tests that check a variety of both simple and complex scenarios, including simulating millions of DHCP clients, thousands of subnets, millions of reservations, and more. We now provide native packages for many operating systems that greatly simplify the installation effort.

ISC DHCP

2021 was not a highly productive year for ISC DHCP. With our DHCP engineering resources fully dedicated to general Kea work, GSS-TSIG, and rapidly increasing user requests for Stork, we decided to focus on these newer projects rather than the legacy ISC DHCP. Nevertheless, in early 2022 we will release ISC DHCP 4.4.3, which will be the last release with both the client and relay components. While this version will be finished in 2022, much of the preparation for it was done in late 2021.

Stork

2021 was also a good year for Stork. The team put out nine releases in total, including the 1.0 milestone version in December. While the project is still minuscule compared to Kea, the user base is growing rapidly, reporting bugs and requesting new features. The project has gotten many new features: TLS support; lease inspection; a configuration review module (Stork can now make suggestions about items to improve in Kea configuration files); better Prometheus and Grafana integration with new statistics; a full configuration viewer for Kea; a service configuration “dump” tool with the ability to assemble all the debugging information typically needed by ISC’s support team, such as configuration files, log files, a database dump, the OS/Kea/Stork versions, etc., in one tarball; and many more. We now have a more-or-less complete dashboard for monitoring Kea and are shifting towards making Stork capable of configuring Kea.

As of the end of 2021, Stork had just over 123,000 lines of code. The team closed 161 GitLab issues in 2021.

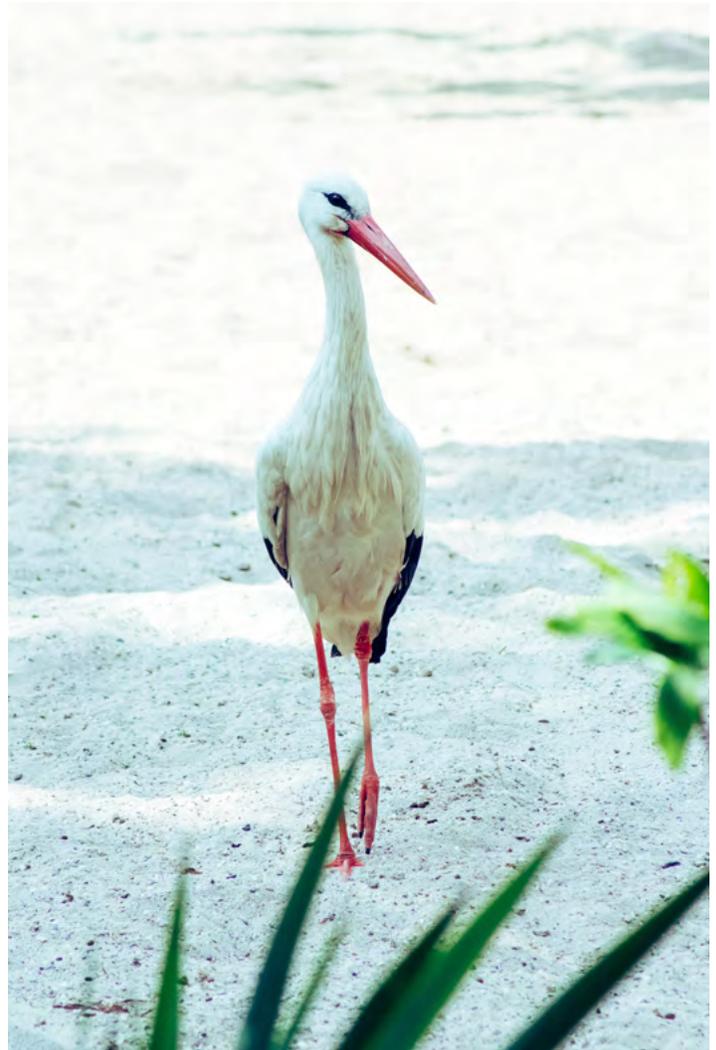


Photo by [Dana Taberima](#) on [Unsplash](#)

SOFTWARE SUPPORT

ISC's revenues come primarily from support services for our software products. At the end of 2021, ISC had 160 customer support contracts representing 139 distinct customers, an increase of eight contracts and six customers compared to the end of 2020. (Some of our customers purchase support contracts for more than one ISC software package.) Only six customers chose not to renew their subscriptions with us in 2021.

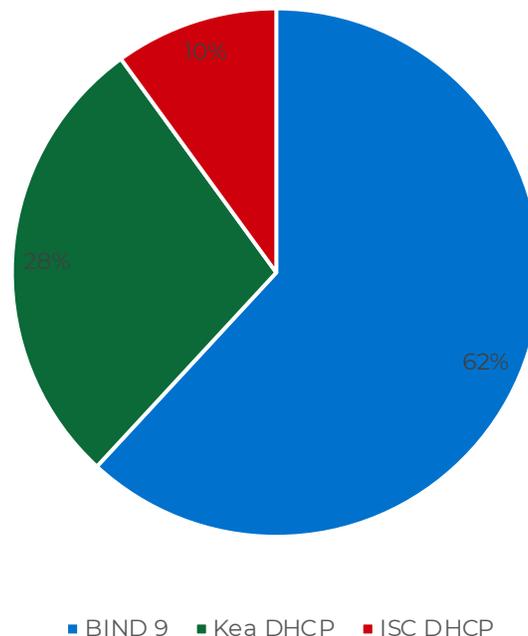
BIND 9 support is our most popular product, but in 2021 we saw significant growth in the number of support contracts for the Kea DHCP server.

The support team changed significantly in 2021, with a new manager and a doubling of the number of support engineers, from three to six.

Here are some of the support team's accomplishments from 2021:

- We reduced the median age of active support tickets by 78% in the second half of the year.
- We revamped our configuration review process to make it more timely and manageable for customers.
- We increased our use of Zoom for customer meetings, instead of relying nearly exclusively on email.
- The team managed five CVE (security vulnerability) cycles and four Operational Notifications.
- The team handled 440 support tickets.
- In the last six months of 2021, we had 231,354 views of our Knowledgebase (KB) at <https://kb.isc.org>.
- We published 33 new KB articles and updated more than 150 others. We added SEO text to all of the articles to improve their searchability via the Internet.

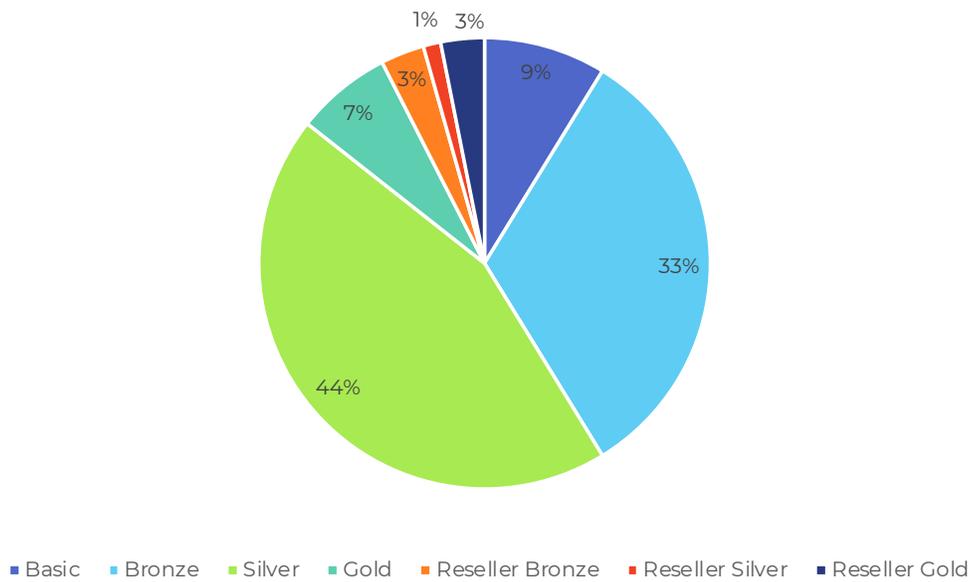
Support Contracts by Product
(as of 12/31/21)



More than half of our enterprise customers opt for the Silver or Gold support level, which includes 24x7 response to critical issues and premium software for BIND 9 subscribers. All Kea support subscribers also get access to premium software.

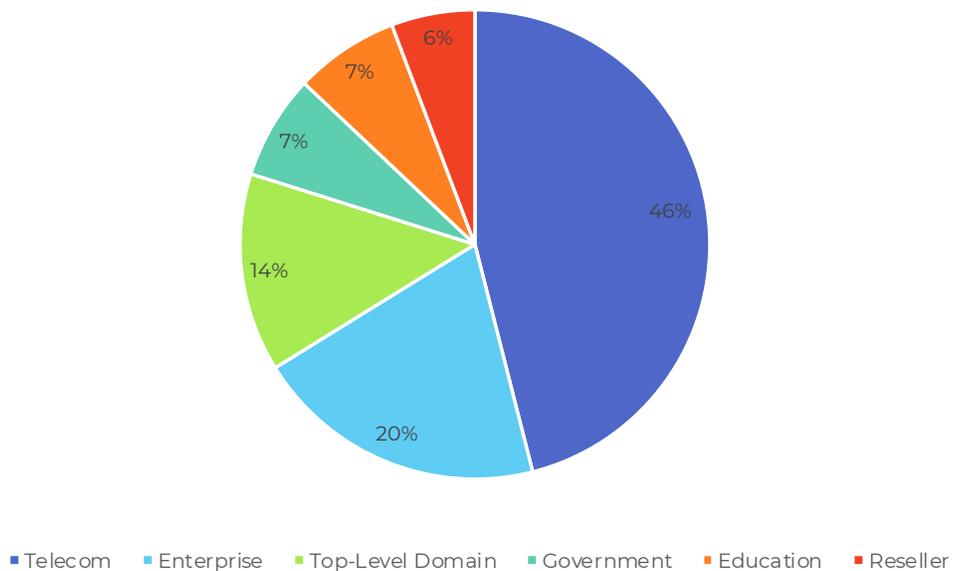
Many open source users tell us that they need the option of premium software to justify paying for technical support.

**Support Contracts by Service Level
(as of 12/31/21)**



Most of our customers are telecommunications companies, enterprises, or top-level domains.

**Support Contracts by Industry
(as of 12/31/21)**



F-ROOT AND TECHNICAL OPERATIONS

Despite the Covid-19 pandemic lasting far longer than anyone hoped - especially since node deployment depends on people actually being physically present in data centers to rack up and connect the hardware - 2021 was a good year for F-Root. We deployed “F-single” nodes at nine new locations, and upgraded “classic” installations to F-single configuration at a further eight locations.

As of the end of 2021, F-Root consisted of:

- 3 “global” sites (at the end of 2020, there were 3)
- 58 F-single sites (2020: 42)
- 8 classic sites (2020: 16)
- 215+ additional nodes hosted by Cloudflare

The global sites host 2x F-Root servers as well as F-Root management infrastructure. An F-single is our current base configuration, which relies on a single 1U server to provide both the F-Root service and BGP Anycast. A classic site comprises 2x F-Root servers, a console server, routers, and switches. The classic sites are all expected to be phased out and upgraded to the F-single configuration by the end of 2022; we have a strong pipeline of new installations and upgrades due as well.

To see a list of all the current F-Root nodes, visit <https://www.root-servers.org/> and select F from the Root Servers list.

Our provisioning systems continue to evolve, with lots of effort going into ensuring the consistency of deployments and to improve our monitoring capabilities. Developing improvements to our system monitoring will continue to be the main focus during 2022, in addition to actual node deployments.

Site Changes Completed in 2021

New Sites

Code	Location	Sponsor
ABQ1	Albuquerque, NM	US NMIX
AGP1	Malaga, ES	Startnix
CCU1	Kolkata, IN	IIFON
DAD1	Da Nang, VN	VNNIC
DEN2	Denver, CO, US	Peaktera
PAH1	Paducah, KY, US	PIE
RIC1	Richmond, VA, US	Ninja-IX
SCL2	Santiago, CL	PIT
TAS1	Tashkent, UZ	SNS-IX

Upgraded Sites

Code	Location	Sponsor
AKL1	Auckland, NZ	InternetNZ
FRA1	Frankfurt, DE	DE-CIX
GRU1	São Paulo, BR	NIC.BR
LIS1	Lisbon, PT	DNS PT
OSL1	Oslo, NO	NIX
PRG1	Prague, CZ	ISC / Peering.cz
SCL1	Santiago, CL	NIC.CL
TPE1	Taipei, TW	CWT

THE PEOPLE OF ISC

Internet Systems Consortium refers to Internet Systems Consortium, Inc. (a not-for-profit company) and its wholly owned subsidiary Internet Systems Corporation, both incorporated in Delaware with headquarters in New Hampshire, USA. Internet Systems Consortium, Inc. is a nonprofit corporation under US IRC 501(c)(3) with the status of public charity under IRC 509(a)(1) and 170(b)(1)(A)(vi). Its US Federal EIN is 20-0141248.

Board of Directors

ISC's Board of Directors is currently made up of four members, each with a long and important history of involvement with the Internet: Rick Adams (Chairman of the Board), Fred Baker (Director), David J. Farber (Director), and Stephen Wolff (Director).

Management

ISC is currently managed by Jeff Osborn (President), Ondřej Surý (Director of DNS Development), Tomek Mrugalski (Director of DHCP Development), Ray Bellis (Director of DNS Operations), Michał Kępień (BIND 9 Quality Assurance Manager), Chuck Stearns (Director of Technical Support), Vicky Risk (Director of Marketing and Product Marketing), T. Marc Jones (Director of Sales), and Jacob D'Erasmus (Director of Finance). Robert Carolina is our General Counsel.

Professional Affiliations

ISC staff continue to participate vigorously in DNS community events and organizations.

In 2021, Ondřej Surý's two-year term on the Board of Directors of the DNS Operations, Analysis, and Research Center ([DNS-OARC](#)) ended, while Ray Bellis was elected to that body. ISC is a "Silver" member of DNS-OARC.

ISC participates in the Internet Corporation for Assigned Names and Numbers ([ICANN](#)) Root Server System Advisory Committee (RSSAC). Ondřej Surý is one of the seven Recovery Key Share Holders for Root Zone DNSSEC Keys, a member of The Registry Services Technical Evaluation Panel (RSTEP), and a member of the RSSAC. Jeff Osborn and Fred Baker have served on the RSSAC since 2017; since 2018, Fred has been co-chair and then chair of RSSAC, and Jeff is the chair of the RSSAC Caucus Membership Committee. Ray Bellis,

Rob Carolina, and Dan Mahoney are also members of the RSSAC Caucus. Petr Špaček is serving a two-year term on the ICANN Technical Liaison Group.

In 2021, Petr Špaček also became a designated expert for the DNS CLASS registry of the Internet Assigned Numbers Authority (IANA).

The Internet Society ([ISOC](#)) promotes the open development, evolution, and use of the Internet for the benefit of all people throughout the world. The work is mainly focused on influencing policy and education, and ISOC is the umbrella organization for the Internet Engineering Task Force ([IETF](#)). Jeff Osborn served as the ISC delegate to the Organization Members Advisory Council (OMAC) from 2015- 2020; David Farber, one of ISC's directors, served as a trustee of the Internet Society.

ISC's engineers attend every IETF meeting and participate vigorously in the development of new standards. Fred Baker serves as chair of the IPv6 Operations (v6ops) group.

Réseaux IP Européens ([RIPE](#), French for "European IP Networks") is the RIR responsible for Europe and the Middle East. RIPE is also a Root System Operators peer, as they operate K-Root. ISC hosts a RIPE Atlas Anchor and a RIPE Routing Collector at its datacenter in Palo Alto, and ISC technical staff participate in RIPE community meetings. Ondřej Surý is a RIPE arbiter.

Cathy Almond is a member of the Communications Committee for the UK Network Operators Forum ([UKNOF](#)), while Ray Bellis serves on its Advisory Council.

Eddy Winstead is a member of the North American Network Operators' Group ([NANOG](#)) program committee, and co-chair of its Outreach program.

Contributions to Other Projects

Ondřej Surý has been providing [Debian packages for PHP](#) for many years; he also commits improvements to [libuv](#).

Michał Kępień implemented a [small feature in tig \(text-mode interface for git\)](#).

Petr Špaček made a variety of contributions to five different open source projects:

- [dnsperf \(DNS Performance Testing Tool\)](#)

- [dnscjit \(an engine for DNS data manipulation\)](#)
- [packetq \(an SQL frontend to PCAP files\)](#)
- [dumdund \(a high-performance DNS server which drops or echoes packets\)](#)
- [DNS Shotgun \(a high-performance, realistic DNS benchmarking tool\)](#)

Dan Mahoney performs release engineering and wrangles tickets for the [Trusted Domain Project's OpenDMARC software](#).

ISC hosts a server for the [University of Oregon Route Views Project](#).

Public Webinars and Presentations

We held and recorded nine technical webinars to provide ongoing training to our users, and ISC staff gave six conference talks, all of which are archived on ISC's [website](#). We would like to thank Carsten Strotmann for being our guest webinar presenter this year.

In addition to posting the recordings on ISC's [YouTube channel](#), we also created a [BrightTalk channel](#) to promote our recordings to a wider audience.

Other Activities of Note

We posted 27 ISC [blogs](#), and we published the [2020 Annual Report](#). We also updated and re-published the ISC timeline on the [About Us page of our website](#). And we had a lot of fun creating an [interactive holiday card](#) this year!

We launched the [ISC swag store](#), using Shopify and Printful to sell and create some fun ISC-branded items.

Since we couldn't meet in person, we tried to keep our morale up with some fun staff team-building activities, like a guess-the-baby-photo contest. The winners got free ISC swag!

ISC donated to several non-profit network operators' groups, as well as to Kea conservation in New Zealand, showing our support for some important organizations.



Check out our ISC Timeline!

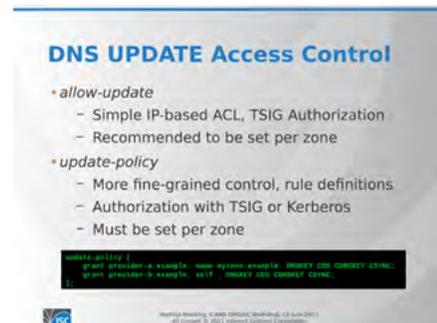
Thank you for supporting ISC's open source! Your purchase supports our nonprofit mission.



Show your love for ISC and open source with a purchase from our swag store!



Got any idea who this little angel might be?



Not many in-person events in 2021, but we did what we could.

OUR CONTRIBUTORS

In some past years, we have simply been unable to keep up with the number of externally created issues. In 2021, we did some impressive catching-up on that front.

We don't always fix the issues reported, if the software version is old or if we disagree with the user's interpretation, or if the benefit is limited compared to the effort. However, in 2021, we fixed more than 80 issues reported by open source users through our GitLab.

We are especially grateful to reporters who:

- Submit issue reports for problems that exist in currently supported software versions
- Test the development branch so we can find and fix issues before they end up in a stable version
- Include logs, crash dumps, and relevant configuration
- Answer followup questions from the developers attempting to root cause the issue
- Verify the fixes we produce
- Provide a patch or suggest a fix

Here are some of the technical contributors from the user community whose reports improved BIND in 2021:

-  Adrien Bernard - reported a bug
-  Alexander Sulfran - reported a regression in check-names
-  Anand Buddhdev - pointed out a documentation error
-  Andrej Podzimek - found a bug in RNDC 9.17.16
-  Andrey Blokhintsev - reported an issue with AXFR under FreeBSD and validated the fix for us
-  Andrey Blokhintsev and (several others) - reported an assertion failure which was published as CVE-2021-25218
-  Benjamin Gentil - reported a deadlock in rndc in 9.11
-  Bhargava Shastry - poked us to use Google's OSS-fuzz program
-  Carl Byington - found a bug in versions 9.16.13, 9.16.13-S1, 9.16.14, 9.16.14-S1, 9.17.11, and 9.17.12
-  Cesar Kuroiwa - provided extensive help in reproducing a crash in XFR over TLS

-  Chris Caputo - tested our libuv integration in the development branch and proposed a logging change
-  Chris Malton - submitted an excellent bug report on IDN support, which led to a fix with help from Tim Rühnen from libidn2
-  Damir Islamov - encountered a problem when upgrading and provided all the information we needed to find and fix it
-  Daniel Stirnimann - found several bugs in the KASP feature, did repeated testing, and validated fixes. Daniel also pinpointed a performance issue with dnssec-verify, and in general is a very helpful DNSSEC tester
-  David Ford - reported a compile issue
-  David M Walker - reported a build failure that was fixed
-  Egbert - found a bug in 9.16.15
-  Erich Eckner - reported an issue with AXFR in 9.16.12
-  Flindeberg - submitted a memorable enhancement request, although we opted not to act on it
-  Friedlho - reported a dig crash
-  Greg Rabil - uncovered an issue with static linking and OpenSSL
-  Hakan Gustafsson - reported an issue with updating signed zones
-  Håvard Eidnes - reported some "impossible" statistics and along with Cathal Mooney tracked the issue for quite a while until it was finally fixed
-  Jean-Christophe Manciot - reported a journal bug that we fixed in the April releases
-  Jean-Christophe Manciot & Vladimir B. Vinogradov - identified a permissions issue causing their installs to fail
-  Jim Pirzyk - reported a bug in dig
-  Jim Popovitch - identified some packet fragmentation issues
-  Jim Westfall - created a confidential issue around memory locking that was fixed in early 2021
-  Jinmei Tatuya - contributed a patch to make the BIND plug-in function asynchronous
-  John Heasley - went above and beyond reporting a complex bug with a lot of followup
-  John Perone - found a bug in the 9.17 development branch

- 🐱 John W. O'Brien - pointed out a documentation bug in auto-dnssec
- 🐱 Josh Soref - reported a documentation bug, probably introduced when we reformatted for RST
- 🐱 JP Mens - reported a usability issue we addressed (and a couple we didn't)
- 🐱 Klaus Darilion - created a confidential issue with AXFR in 9.16.2
- 🐱 Kris Karas - found and verified the fix for a deadlock in 9.16.18 and sparked a discussion about integrating NSEC3 into dnssec-policy
- 🐱 Laurent Frigault - submitted a crash dump with all the information we needed to find and fix it
- 🐱 Laurent Gouhier - reported a performance loss in 9.16
- 🐱 Legacy1 - reported a Windows issue, which Richard Neal reproduced for us
- 🐱 LM Jogbäck - found an issue with dnssec-policy
- 🐱 Lusia Kundel - submitted a typo fix in nsupdate help
- 🐱 Marc Dequènes (Duck) - reported several issues with dnssec-policy and tested the fixes (Quack!)
- 🐱 Mathieu Arnold - reported an issue that was first logged with FreeBSD. Several other BSD users chimed in, including Xin Li and Dimitry Andric, until John W. O'Brien confirmed that the issue had been fixed in a later release
- 🐱 Michael Osipov - reported a bug in a test, which was fixed, then found yet another problem with Kerberos linking, and also found an issue with nsupdate
- 🐱 Michel Lespinasse - reported an issue with DNSSEC key rotation with multiple views
- 🐱 Ole Bjørn Hessen - reported that BIND 9.16.8 does not honor CPU affinity
- 🐱 Oskar Stenman - noticed that "masters" were not renamed to "primaries" in CATZ
- 🐱 Patrick McLean - submitted a patch to improve dig's timestamp accuracy
- 🐱 Pdw-mb - found a documentation error
- 🐱 Per Lundberg - added to an existing bug report instead of creating a new one (thank you for this!)
- 🐱 Petr Menšík of RedHat - made many contributions throughout the year, including several merge requests
- 🐱 Phil Regnauld - pointed out a typo in the DNSSEC Guide
- 🐱 Piolink-kycho - found a memory leak during stress testing
- 🐱 Rainer W. - provided a bug report with suggested fixes
- 🐱 Ralf Jung - reported an issue with inline signing, confirmed by Jean-Christophe Manciot
- 🐱 Richard Laager - found an interoperability issue we ended up deciding not to add a workaround for, but which we appreciated
- 🐱 Roland Illig - took the time to report a minor documentation typo
- 🐱 Rosen Penev - submitted a patch
- 🐱 Sara Dickinson - helped in testing and specifying requirements for XoT
- 🐱 Sean Zhang - found and correctly diagnosed the infamous issue with the missing "w" that resulted in security fixes across all supported versions in June
- 🐱 Stacey Marshall - reported a Solaris configuration issue
- 🐱 Stanislav Levin - found a problem with the cache for managed keys in 9.16
- 🐱 Stuart Henderson - reported an obscure test issue with OpenBSD and Raspbian
- 🐱 Sven Strickroth - suggested an additional log message to improve usability
- 🐱 Thomas Amgarten - found a tricky issue with journal files
- 🐱 Thomas Amgarten - helped us with KASP troubleshooting
- 🐱 Timothe Litt - highlighted the use of http references in the documentation
- 🐱 Tobias Günther - prompted us to update Launchpad for new Ubuntu versions
- 🐱 Triatic - tested BIND's DoH implementation vs. Windows
- 🐱 Vsevolod Volkov - observed a memory leak on FreeBSD and verified the fix for us
- 🐱 Wil Knoll - reported a bug in QNAME minimization

We also offer our thanks to:

- Our stalwart ISC DHCP community experts Simon Hobson, Sten Carlsen, Bill Shirley, Bob Harold, Niall O'Reilly, Glen Satchell, and Gregory Sloop, who are helping a whole new generation of users with their ISC DHCP issues via the dhcp-users mailing list.
- Numerous other BIND users, Kea users, and ISC DHCP users, who provided expert advice to others on our user mailing lists. ISC staff could not possibly answer all these questions ourselves, not only because of the number of questions, but because we don't have the depth and variety of operational experience our users have. We are grateful for these contributions of technical expertise.
- The many sponsors of our F-Root nodes. They donate rack space, purchase servers, help support our operating costs, and generally make it possible to provide free root services to the Internet.



Photo by [Howie R](#) on [Unsplash](#)

Thank you for reading our 2021 Annual Report, and for being part of the open source community. We look forward to continuing to serve you for many years to come.

Does your company or organization use ISC software? If you're not already a customer, please consider purchasing an ISC support contract. Paid support contracts provide our funding so we can continue our important work of keeping the Internet open and available to everyone. Please visit <https://www.isc.org/support> to find out more.

You can also show your support for open source by purchasing items from our swag store! Check it out at <https://shop.isc.org>.

