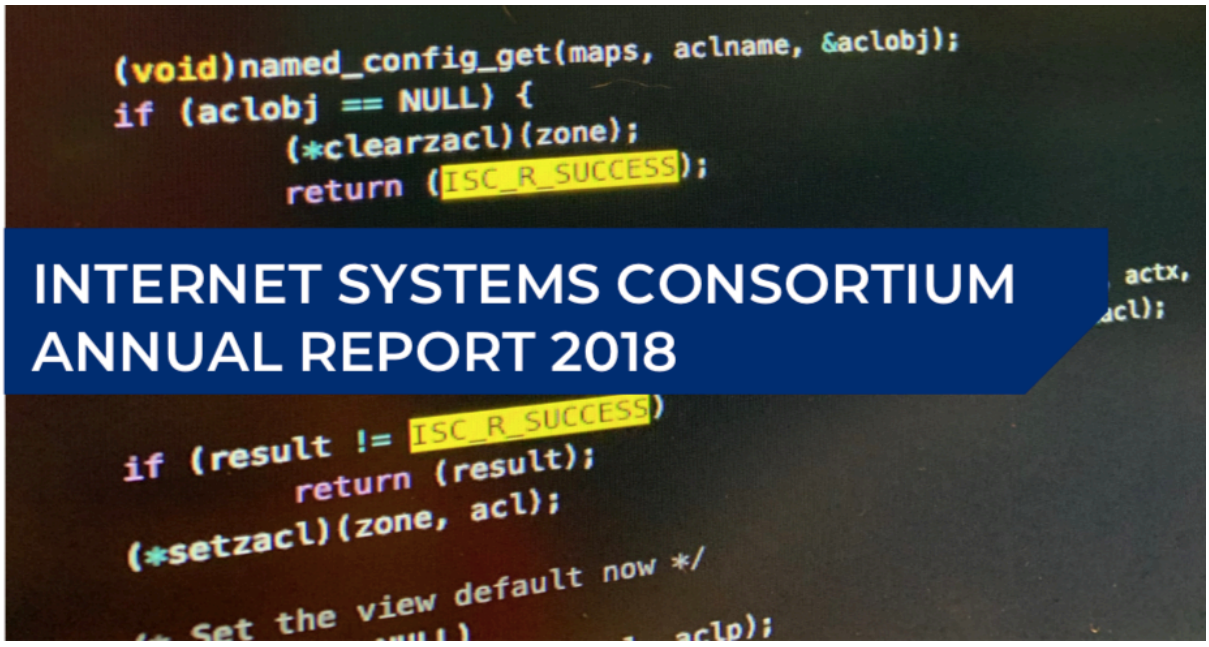
From: **Internet Systems Consortium** info@isc.org
Subject: Latest News about your ISC Support Subscription
Date: July 23, 2019 at 7:16 AM
To: vicky risk vicky@isc.org

IC

ISC Support Subscriber News

2019 Q3

This quarterly newsletter brings updates and inside information to ISC's BIND 9, ISC DHCP, and Kea DHCP support subscribers. We hope you find it useful.



ISC News

We hope you are proud to be supporting ISC - read ISC's 2018

ISC is hiring! We are interviewing now for a BIND 9 Developer and a

annual report.

If you haven't looked at ISC's website in a while, you're in for a big surprise. This new static site should be faster, and much less vulnerable to infection and attack. We have also removed all Google tracking tags and cookies for your privacy.

QA Engineer. Encourage your friends to apply!

ISC's Matthijs Mekking was interviewed about the BIND and Kea roadmaps in this Men and Mice podcast.

Listen---> at the links below, or on ITunes: https://hubs.ly/H0jw8sx0

SoundCloud Spotify RSS

BIND/DNS News

GeoIP2.0

BIND 9's GeoIP support has been updated to work with the new GeoLite2 API from Maxmind. This new API was added in 9.15.2, and backported to 9.14.4 and 9.11.9.

Change is (Sometimes) Good

We have a new BIND 9 policy on removing obsolete features, created following a fairly vigorous discussion on the bind-users mailing list.

Flag Day Cometh Again

A second DNS Flag Day is planned

A second DNS Flag Day is planned for sometime in 2020, to focus on reducing reliance on packet fragmentation and improving access to TCP for large packets. We have tested the primary domain for each of our subscribers and we will let you know if we spot a potential issue there. (If you haven't heard from us about this yet, then we didn't spot a problem with your primary domain.)

FASTer RPZ Plug-in Available

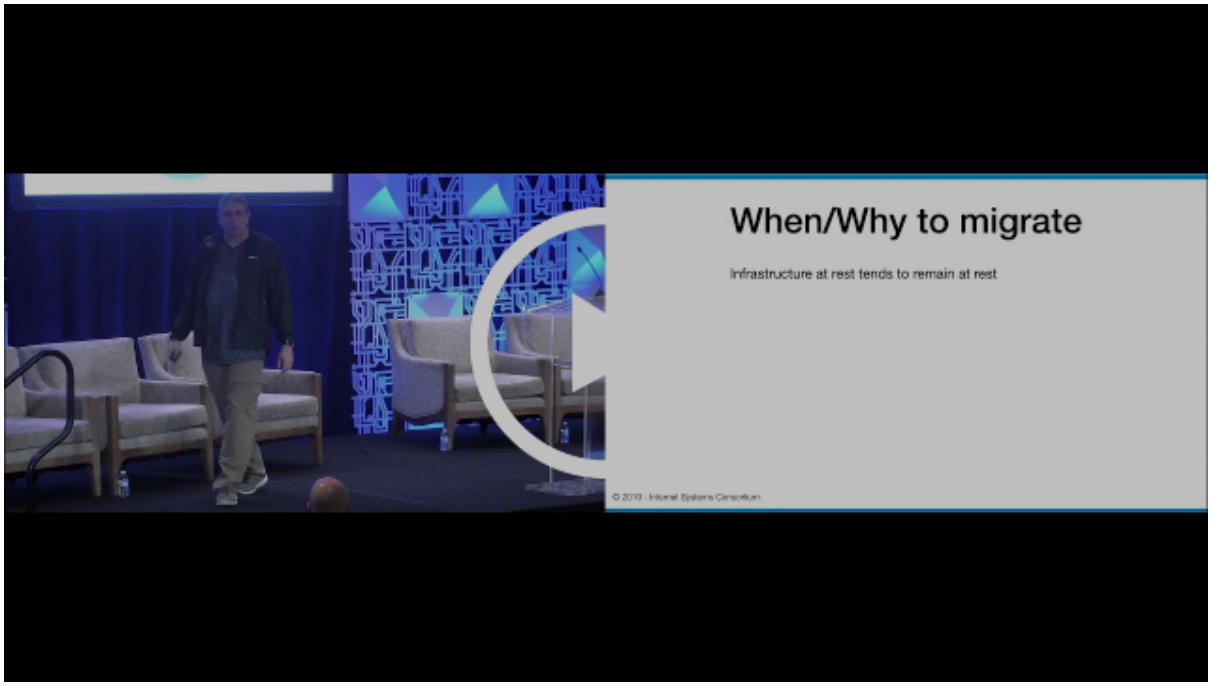
Farsight's RPZ application using BIND's Response Policy Service interface loads even faster than the refactored BIND-native RPZ. Farsight is generously offering the plug-in free to ISC BIND support subscribers, and it works with any vendor's RPZ zones. Contact ISC support to be added to Farsight's list of eligible accounts. Read more at https://www.farsightsecurity.com/technical/fastrpz/.

Kea/DHCP News

How will you use your new powers?

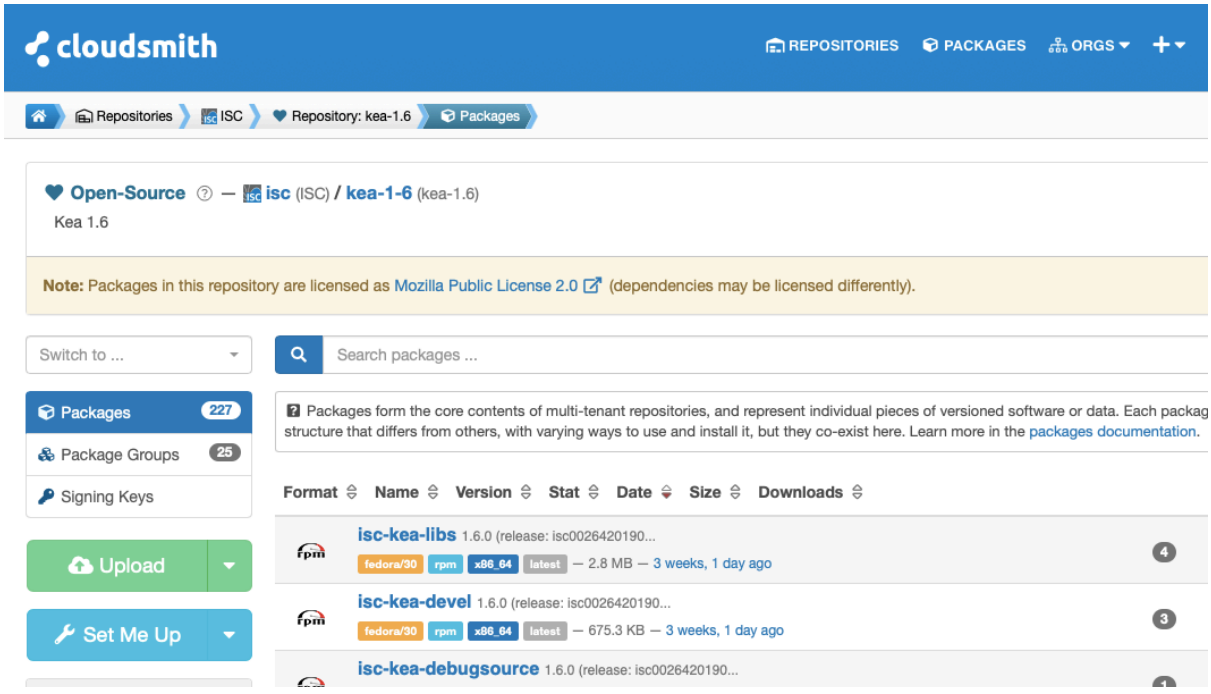
Kea 1.6.0 is in beta testing now, with a release planned in late August. This release adds the very powerful ability to manage your Kea server

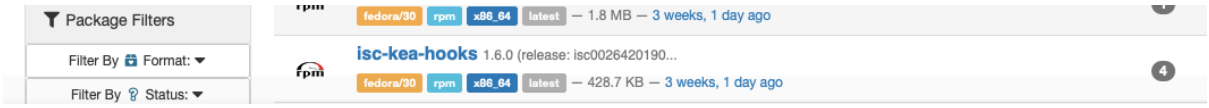
configurations in a database backend. Register here for a webinar on August 14th, 2019, on "Using the Kea Configuration Backend."



Scarred by past network migrations

WATCH --> ISC's Alan Clegg at NANOG on "Migrating from ISC DHCP to Kea"





NEW ISC Binary Package Repository (Yay!!!)

In response to MANY REQUESTS, we have been busy building packaged versions of our software. BIND 9 open source packages from ISC are available now on Launchpad, and the Fedora copr. We recently established a repository for Kea packages, including our premium software.

Kea support subscribers should have received a ticket with a unique per-organization access code for premium packages in our repository on Cloudsmith.io. Kea subscribers now have access to 467 ISC-supported binaries for RHel, Centos, Debian, and Ubuntu. We will be adding packages for the BIND 9 Subscription Edition to Cloudsmith and when those are ready, we will notify eligible subscribers via a ticket.

Proposed Change in Policy to Reduce Unnecessary CVEs

ISC has followed a publicly available Software Defect and Security Vulnerability Disclosure Policy for years, and we are proud of our record of integrity in adhering to our published policy. However, increasingly we've become convinced that it is time to make some changes to that policy in response to feedback from our customers and to adapt to new software release policies which result in smaller, more frequent maintenance releases. Additionally, due to the rigidity of the existing policy we have found ourselves spending a lot of our resources on, and issuing some CVEs for, problems we think do not really impact many - or any - of our users. For these and other reasons, we are considering updating our policy. This change, if we make it, should reduce the frequency of unplanned emergency updates for our users while allowing our organization the discretion to issue vulnerability disclosures if we feel the operational risk of an issue justifies one regardless of its CVSS score.

Why Make This Change?

It is not just a matter of the inconvenience to the development team at ISC. When we issue a CVE, that triggers mandatory actions for a whole downstream ecosystem, including packagers, independent software vendors, and organizations that use our software. At a minimum, they have to evaluate the potential impact of the vulnerability, if not perform emergency software releases and system updates. We already try to schedule vulnerability announcements for mid-week, to avoid causing weekend emergencies for our users, but we wanted to assess what else we could do to reduce the incidence of "non-critical" software vulnerability announcements.

The vast majority of our BIND 9 security vulnerabilities have been denial of service (DoS) bugs: ways to cause BIND to exit, typically by violating a "software contract." (71% or 67 of 98 reported vulnerabilities in BIND 9 were DoS vectors, according to CVE Details.) BIND is designed to react by terminating when it encounters unexpected or illegal conditions, because this is considered safer than continuing to operate in an unknown state.

Obscure Configuration Scenarios

The Common Vulnerability Scoring System (CVSS) that we use to assess the severity of potential security vulnerabilities is a widely-used industry standard but it has some significant limitations. Because it does not take into consideration entire classes of context information, bugs which score similarly may in fact be wildly different in expected real-world impact. It is not uncommon for a vulnerability which we expect to present little real-world practical impact to score a higher CVSS severity than a more realistically exploitable vulnerability, due solely to the weighting of factors used by the scoring system.

One example, from about a year ago, is CVE-2018-5740: A flaw in the "deny-answer-aliases" feature can cause an assertion failure in named. This was a bug that would have made it virtually impossible to operate a server with this obscure feature (deny-answer-aliases) turned on, but the feature was extremely unlikely to be used. So unlikely that, despite the fact that it would be hard to keep a server up for more than 10 minutes if you were using it, nobody had ever reported the problem to us because as far as we could tell literally nobody had ever used that feature (or if they had, their server had crashed within 10 minutes and they had turned it off again).

Because of the way that CVSS scores things we had to issue this as a Severity: High vulnerability, even though (at a very conservative estimate) fewer than 1 in 10,000 or 100,000 operators would be vulnerable to it. This is a good example of the sort of very obscure operating condition that we think mitigates the need to declare a CVE. (If you have a suggestion for a general rule that would except obscure deployment scenarios from our security policy, we would love to hear it.)

Medium or High Severity?

Our current policy relies on the BASE CVSS score. The CVSS system defines an issue that scores from 4.0 - 6.9 on this scale as a "Medium" severity. However, for years, ISC has treated any bug that scores above 5.0 on the base CVSS factors (based on Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, Confidentiality, Integrity, Availability) as serious enough to trigger an Advance Security Notification to our support subscribers and DNS root operators, followed by a -P patch release and publication of a CVE.

CVEs only for High-Severity and Critical Issues

The change we could make that would have the biggest impact would be to raise the threshold at which our process will *require* issuance of a CVE and an out of cycle -P maintenance release. We are considering raising that threshold from the current 5.0 score to 7.0. This is more in line with the CVSS characterization of issues scoring between 5 and 7 as "medium severity," and issues scoring 7 and above as "high severity."

Under the proposed new policy, security issues scoring below 7.0 would be evaluated by us, using our own judgement to weigh factors not considered by the CVSS scale. Some bugs, if we felt the real-world risk to operators was low, could be treated like non-critical security bugs. Other bugs might be treated as they are currently, with an out-of-cycle security patch release and scheduled public disclosure to operators. In between there might be yet another category that would be treated as confidential until our next maintenance release and

then disclosed when a public fix is ready.

If you have any feedback, suggestions or concerns about the proposed change to our policy for handling security bugs, please open an issue with us to discuss them. We would love to know what you think about this important topic.
