Open source risks: perception & mitigation Petr Špaček, Victoria Risk 2024-05-23 pspacek@isc.org, vicky@isc.org

Experimental session

- Survey
- BIND 9 DNS server
 - as an example project
- Discussion

Survey

https://ec.europa.eu/eusurvey/publication/ RIPE88OpenSourceWGSurvey

Survey

- What makes a project trustworthy?
 - "Software you consider mission critical in your deployment"
- Secure deployment practices
- Risk mitigation practices

Survey

- Audience bias
- Operators "who care"
- Presumably experts
 - RIPE Open source WG
 - RIPE DNS WG
 - dns-operations list @ DNS-OARC
 - Internet Systems Consortium's public channels

• 71 answers

Mission critical software



How do you build confidence? #1



How do you build confidence? #2

How do you verify signatures?

How do you install software?

How do you mitigate upgrade risks?

How do you test before production?

A DNS server – example project

BIND 9 in numbers

First commit	1998	26 years ago!
C code	263 000	lines (w/o tests or comments)
Automake	3 143	lines
Autoconf	1 839	lines
M4	1 626	lines
# of authors	50+	in the current codebase
# config knobs	325+	some are context dependent
# CVEs	130	mostly DoS

* attribution of old code is hard – squash & merge model

Existing code – audit

- Who knows what's in there?!
 - 26 years!
- Security audit in 2023
 - https://www.isc.org/blogs/2024-bind-audit/
 - 1 CVE, 2 medium severity, 6 low, 23 "nits" ...
 - Low-level bugs

Audit limits

- No DNS-protocol level bugs found
 - By auditors non-DNS experts
 - Meanwhile ...

CVE #	Short Description
2023-50868	Preparing an NSEC3 closest encloser proof can exhaust CPU resources
2023-50387	KeyTrap - Extreme CPU consumption in DNSSEC validator
2023-6516	Specific recursive query patterns may lead to an out-of-memory condition
2023-5680	Cleaning an ECS-enabled cache may cause excessive CPU load
2023-5679	Enabling both DNS64 and serve-stale may cause an assertion failure
2023-5517	Querying RFC 1918 reverse zones may cause an assertion failure when
2023-4408	Parsing large DNS messages may cause excessive CPU load

BIND 9 vs. survey – CVEs

Self-imposed policies

- Coding & review procedures
- OpenSSF software quality badge openssf best practices passing
 - Lots of non-technical requirements
- ISC software defect and security vulnerability disclosure
- ISC CVSS scoring guidelines
- A lot of invisible work

BIND 9 vs. survey – processes

BIND 9 new code

- Peer review in GitLab
 - Very few external contributions
- Automated tests
 - Continuous integration in GitLab
 - Extra things "on side"

Automated tests

- Unit tests
- Integration
- Fuzzers
- Interoperability
- Stress
- Performance ...

GCC Code Coverage Report

Metric	Coverage					
Lines	77.1 %					
Functions	85.5 %					
Branches	55.6 %					
incl. 12 204 assertions,						
65.3 % with	out them ²³					

Continuous integration

autoconf	precheck	build	unit	system	performance	doca	postcheck	Downstream						
@ sutorecont	O black	Clangcasan	o unticlangrasan	eross-version-config-tests	Intgundet	e docs	🖉 hck	bind9-shotgun-ci						
	C changes	Clangsbookworm amd 64	unit clang bookworm and 64	💿 respd#) (o shotgunitop	docatarbal	(goov	hindlishting.cl	jobgen	performance	Downstream			
	C checkbashisms	Clangibulluryecamd64	💿 unit:clang:bullaeye:amd84	Respective	ahotgunudp		🔵 scan-build	ATTOICES (Multi-project)	C Resolver-shotgun-pipeline-generator	resolver-shotgun-child-pipeline	resolver-shotgun	build	teat	postproc
	C-variables	Clangtheebsd13:amd64	🕑 unit:clang:freebed13:amd64	🖉 respdittasan	atress: authoritative:feciora:40:amd64					(Trigger job)	(Child)	bind-4434011ccc/87d8H54e59467f09dH0d08	@ main	o peatpree
	🥥 clang-format	Clangtheebad14:amd64	unit:clang:freebad14:ared64	🖉 respdittsan	atress authoritative:teclora:40.arm64							@ bind-v9.19.23	@ v9.19.23	
	Coccinelle	Clangropenbad amd64	unit:clang.openbad:amd64	Ø system clang asan	stress authoritativectreebod13:amd64			bind9-shotgun-cl #170266						
	🖉 mise	Cangtuan	@ unit:clangtaan	Ø system clang bookworm and 64	stress:recursive:fedors:40:amd84			Multiproject						
	💿 туру	gcc:59(ps:amd64	Junit:gcc.81px and 54	System clang trails eye and 54	e stress:recursive:fedors:40:am84									
	O pyint	gcc:Pfps:amd84	Integec9tipsand64	System clang freebod13 and 64	atress recursive freebad12 and 64									
	C PELER	gcc:alpine3.19camd64	@ unit:gccalpine3.19 amd64	system:clangfreebad14.amd64	Ø stress:rpz:fedors:40:ared64									
	Shifest	@ gec:asan	O untrpccasar	💿 systemclangtaan	@ stress:rpz:fedors:40:arm64									
	C tarbali-create	gcc:bookworm:amd64	o unit:gcc:bookworm:amd64	system: gcc:8ftps: and64	🖉 stress:rpz:freebsd13.amd64									
		gcc:bookworm:amd64crass32	i unit:gcc.bookworrcrbit.amd64	👩 system got Stips and 64										
		gcc:bookworm:bt:and64	🕑 unt:gcc.bullsøye and64	🕑 system gcc sipine3.19 and 64										
		gcc:bullesystand64	@ untrgccfocalamd64	Ø system got asan										
		@ gcc:focal.amd84	@ unt:gccjammy:amd64	@ system.goc.bookworm.and64										
		@ gcc:jammy:amd84	@ unt:gcc.noblexamd64	System got bookworm rbt and64										
		gcc:noble:amd64	i unit:gcc.oraclelinuxit:amd64	👩 system god bullarye and 64										
		gcc:oraclelinus8:ared54	unit:gcc.tracklinux9tamd64	System gcc.focal.amd64										
		gcc:oraclelinusRamd54	O untrgccoul3amd64	System gozjam my amd 64										
		gc::ossi3:sidamd64												
		@ gcc:out-of-tree	o K											
		acc: ald arrid\$4	or mai	1										
		C gettantaatrioaprinx				~								
		C geenan	Schedul	ed CO	112 iobs	(0)	69 m	inute	s 53 sec	conds o	llelle	d for 14 🤉	seco	nds
		C get unterweet and o	ochedu	u u	112 1000			mace			lacac			190
		Darwine .												
											_			
			Pinelir	ne Ni	shae	Johs	: 112	7	Failed . I	obs 1	Te	ets 632	1	
			i ipeui		0000	0003		-			10	002		

BIND 9 vs. survey – tests

Peer review

Peer review

16 files +141 -383

28

📗 📧 ISC Open Source Projects / 🎯 BIND / Merge requests / **!5071**

‰ Merged	use a fixedname bu	ffer in dns_message_g	gettempname() 2515-improve-glue-cache-p	e [^e] into main
Overview (Commits 2	Pipelines 6 Ch	anges 16	
Q Search (e.g. *.vue) (Ct	rl+P)	✓ lib/dns/rbtdk	D.C [^{o1}	
นแร		9927 -	0xfc, 0xfd, 0xfe, 0xff	
		9888 + s	tatic const unsigned char maptoupper[25	6] = {
include/dns		9889 +	['a'] = 'A', ['b'] = 'B', ['c'] :	= 'C', ['d'] = 'D', ['e'] = 'E',
h message.h	+3 -20 💽	9890 +	['f'] = 'F', ['g'] = 'G', ['h'] :	= 'H', ['i'] = 'I', ['j'] = 'J',
		9891 +	['k'] = 'K', ['l'] = 'L', ['m'] :	= 'M', ['n'] = 'N', ['o'] = 'O',
🗁 win32		9892 +	['p'] = 'P', ['q'] = 'Q', ['r'] :	= 'R', ['s'] = 'S', ['t'] = 'T',
🕒 libdns.def.in	+0 -1 💽	9893 +	['U'] = 'U', ['V'] = 'V', ['X'] :	= 'X', ['y'] = 'Y', ['z'] = 'Z',
		9928 9894 }	;	
c message.c	+56 -107 💽			
c rbtdb.c	+40 -129 💿			<pre>const dns_rdataset_t *rdataset, dns_name_t *name) {</pre>
c resolver.c	+0 -1 💿	Q 🗸	Approvo	te1;
		\mathbf{O}^{\star}	ADDIOVE	rivate2;
c tkey.c	+4 -18 💽	-		te3; /* RDATASLAB */
c tsig.c	+3 -6 •			
c xfrin.c	+0 -2 •	9937 -	unsigned char bits;	
C 7000 C	.0.2 🗖	9938 -	unsigned char c, flip;	
C Zone.c	+0 -3 💽	9901 +	rdatasetheader_t *header = NULL;	
🗁 ns		9902 +	<pre>uint8_t mask = (1 << 7);</pre>	
a aliant a		9903 +	<pre>uint8_t bits = 0;</pre>	
c cuent.c	+12 -38 💽	9939 9904		
c query.c +8-21 • 9940 9905 header = (struct rdatasetheader *)(raw - si		*)(raw - sizeof(*header));		
	_	9941 9906		
c xfrout.c	+0 -2 💽	00	-9946,85 +9911,36 @@ rdataset_getowner	case(const dns_rdataset_t *rdataset, dns_name_t *name) ·

Release ... err, try again ...

ISC (https://fosstodon.org/@iscdotorg) @ISCdotORG

Ok, this is embarrassing. Please don't install the @bind9 updated versions we posted yesterday. Someone reported an error - we left out a LETTER of the ALPHABET in a streamlined routine. We will be removing the new versions and reposting after we have a chance to retest.

5:24 AM · Jun 18, 2021

...

Automated tests – limits

🔲 🜆 ISC Open Source Projects / 🎯 BIND / Issues / **#2779**

W or w characters in domain names are altered to "\000"

⊖ Closed
☐ Issue created 2 years ago by Sean Zhang

Summary

We recently upgraded our bind9 from 1:9.16.16-2+ubuntu18.04.1+isc+1 to 1:9.16.17-1+ubuntu21.04.1+isc+1 and start experiencing some wildcard names not being resolved. The resolver will return servfail. After some troubleshooting we found that:

Under certain conditions (reproducible), the name in answer will not match the name in question. Found this issue reproducible with following conditions:

:

Peer review – limits

] 🚾 ISC Open Source Projects / 🌀 BIND / Merge requests / **!5071**

🗞 Merged 🛛 use a fixedname buffer in dns_message_gettempname() 🛛 2515-improve-glue-cache-pe...

Overview 0 Commits 2 Pipelines 6 Changes 16

~	lib/dns/	rbtdb.c [^{e1}
9900		- 0x00,
9901		$- \qquad \qquad$
9902		$ 0 \times 00, 0 \times 00, 0 \times 00$
	9880	<pre>+ static const unsigned char maptolower[256] = {</pre>
	9881	+ ['A'] = 'a', ['B'] = 'b', ['C'] = 'c', ['D'] = 'd', ['E'] = 'e',
	9882	+ ['F'] = 'f', ['G'] = 'g', ['H'] = 'h', ['I'] = 'i', ['J'] = 'j',
	9883	+ ['K'] = 'k', ['L'] = 'l', ['M'] = 'm', ['N'] = 'n', ['0'] = 'o',
	9884	+ ['P'] = 'p', ['Q'] = 'q', ['R'] = 'r', ['S'] = 's', ['T'] = 't',
	9885	+ $['U'] = 'u', ['V'] = 'v', ['X'] = 'x', ['Y'] = 'y', ['Z'] = 'z',$
9903	9886	};
9904	9887	

The matrix is square! It must be fine!

BIND 9 Release process

Release Checklist

Before the Code Freeze

- 🗹 (QA) Rebase -S editions on top of current open-source versions: git checkout bind-9.18-sub && git rebase origin/bind-9.18
- QA) inform Support and Marketing of Impending release (and give estimated release dates).
- (QA) Ensure there are no permanent test failures on any platform. Check public and private scheduled pipelines.
- Q(QA) Check charts from shotgun:* jobs in the scheduled pipelines to verify there is no unexplained performance drop for any protocol.
- (QA) Check Perfab to ensure there has been no unexplained drop in performance for the versions being released.
- QA) Check whether all issues assigned to the release milestone are resolved¹.
- (QA) Ensure that there are no outstanding merge requests in the private repository¹ (Subscription Edition only).
- Q (QA) Ensure all merge requests marked for backporting have been indeed backported.
- (QA) Announce (on Mattermost) that the code freeze is in effect.

Before the Tagging Deadline

- (QA) inspect the current output of the cross-version-config-tests job to verify that no unexpected backward-incompatible change was introduced in the current release cycle.
- Q(QA) Ensure release notes are correct, ask Support and Marketing to check them as well. Example
- (QA) Add a release marker to CHANGES. Examples: 9.18, 9.10
- (QA) Add a release marker to CHANGES.SE (Subscription Edition only). Example
- (QA) Update BIND 9 version in configure.ac (9.18+) or version (9.16).
- Q (QA) Rebuild configure using Autoconf on docs.isc.org (9.16).
- Q(QA) Update GitLab settings for all maintained branches to disallow merging to them: public, private
- QA) Tag the releases in the private repository (git tag -s -n "BIND 9.x.y" v9.x.y).

Before the ASN Deadline (for ASN Releases) or the Public Release Date (for Regular Releases)

- (QA) Check that the formatting is correct for the HTML version of release notes.
- (QA) Check that the formatting of the generated man pages is correct.
- QA) Verify GitLab CI results for the tags created and sign off on the releases to be published.
- O (QA) Update GitLab settings for all maintained branches to allow merging to them again: public, private.
- Q(QA) Prepare (using version_bump.py) and merge MRs resetting the release notes and updating the version string for each maintained branch.
- Q(QA) Rebase the Subscription Edition branches (including recent release prep commits) on top of the open source branches with updated version strings.
- (QA) Announce (on Mattermost) that the code freeze is over.
- QA) Request signatures for the tarbalis, providing their location and checksums. Ask signers on Mattermost.
- (Signers) Ensure that the contents of tarballs and tags are identical.
- (Signers) Validate tarball checksums, sign tarballs, and upload signatures.
- (QA) Verify tarball signatures and check tarball checksums again: Run publish_bind.sh on repolsc.org to pre-publish.
- Q(QA) Prepare the patches/ subdirectory for each security release (if applicable).
- Q(QA) Pre-publish ASN and/or Subscription Edition tarballs so that packages can be built.
- (QA) Build and test ASN and/or Subscription Edition packages (in cloudsmith branch in private repo). Example
- O (Marketing) Prepare and send out ASN emails (as outlined in the CVE checklist; if applicable).

On the Day of Public Release

- O (QA) Wait for clearance from Security Officer to proceed with the public release (if applicable).
- (QA) Place tarballs in public location on FTP site.
- QA) Inform Marketing of the release, providing FTP links for the published tarballs.
- (QA) Use the Printing Press project to prepare a release announcement email.
- (Marketing) Publish links to downloads on ISC website. Example
- (Marketing) Update the BIND -5 Information document in SF with download links to the new versions. (If this is a security release, this will have already been done as part of the ASN process.)
- (Marketing) Update the Current Software Versions document in the SF portal if any stable versions were released.
- (Marketing) Send the release announcement email to the bind-announce mailing list (and to bind-users if a major release example).
- (Marketing) Announce release on social media sites.
- (Marketing) Update Wikipedia entry for BIND.
- (Support) Add the new releases to the vulnerability matrix in the Knowledge Base.
- (Support) Update tickets in case of waiting support customers.
- QA) Build and test any outstanding private packages in private repo. Example
- QA) Build public RPMs. Example connit which triggers Copr builds automatically
- (SwEng) Build Debian/Ubuntu packages.
- (SwEng) Update Docker files here and make sure push is synchronized to GitHub. Docker Hub should pick it up automatically. Example
- Q(QA) Ensure all new tags are annotated and signed. git show --show-signature v9.19.12
- (QA) Push tags for the published releases to the public repository.
- (QA) Using merge_tag.py, merge published release tags back into the their relevant development/maintenance branches.
- (QA) Ensure allow_failure: true is removed from the cross-version-config-tests job if it was set during the current release cycle.
- QQA) Sanitize confidential issues which are assigned to the current release milestone and do not describe a security vulnerability, then make them public.
- Q(QA) Sanitize confidential issues which are assigned to older release milestones and describe security vulnerabilities, then make them public if appropriate².
- QA) Update QA tools used in GitLab CI (e.g. Black, PyLint, Sphinx) by modifying the relevant Dockerfile.
- QA) Run a pipeline to rebuild all images used in GitLab CI.
- (QA) Update netadata.json with the upcoming release information.

BIND 9 release process

- Check list of changes that went in (again)
- Polish docs
- Run tests (again)
- Generate tarball
 - Check reproducibility
- Sign
- Publish
- Build packages

BIND 9 tarball checks

- Git ⇒ tarball reproducibility
 - https://gitlab.isc.org/isc-projects/BIND
 9/-/blob/main/util/release-tarball-comparison.sh
 - 100 lines
 - easy enough for independent review

BIND 9 tarball signing

- Dedicated VM
 - takes tarball from Gitlab
 - requests GPG signature
- Signer person
 - SSH into the VM
 - forwards GPG agent socket

BIND 9 vs. survey – signatures

BIND 9 package build

- Our RPM packages build in Gitlab
- Copr, Launchpad, Docker, etc. manual

BIND 9 vs. survey – packages

BIND 9 team vs. survey							
	Team priority	Survey priority					
CVE frequency	#1	# 8					
CI & automated tests	#1	# 11					
code reviews & standards	#1	# 13					

Discussion

Thank you!

- Main website: https://www.isc.org
- Software downloads: https://www.isc.org/download or https://downloads.isc.org
- Presentations: https://www.isc.org/presentations
- Main GitLab: https://gitlab.isc.org