Open By Default

A year in the life of commercial open source

Open By Default

A year in the life of commercial open source

WHO IS THIS CLOWN?!

CRob, n, adj, and v
Pronunciation: U.S. (K-robe)
Over 20 years of Enterprise-class Architecture, Engineering, Operations, and Security experience
Ambassador of Red Hat Product Security
Participant in the FIRST PSIRT SIG, VulnCoord SIG, and others
Co-Author FIRST PSIRT Services Framework
Pirate-enthusiast & hat-owner

> “This is a quote. Words full of wisdom that someone important said and can make the reader get inspired.”
>
> —SOMEONE FAMOUS

Table of Contents

01 **Introduction**

Why OSS is important

02 **Presentation**

The stuff about the title that draw you
to sit here and listen

03 **Conclusion**

Reflections on the amazing revelations
you have witnessed
during the hour

01

This is a great headline:

OSS Won!

(yay!)

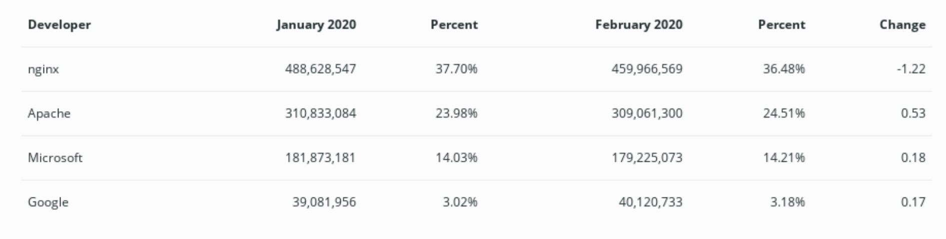
OSS IS KIND OF A BIG DEAL

"FOSS constitutes 80-90% of any given piece of modern software, and software is an increasingly vital resource in nearly all industries. This heavy reliance on FOSS is common in both the public and private sectors, and among tech and non-tech companies alike. Therefore, ensuring the health and security of FOSS is critical to the future of nearly all industries in the modern economy." - Linux Foundation's "Vulnerabilities in the Core" report - Feb2020

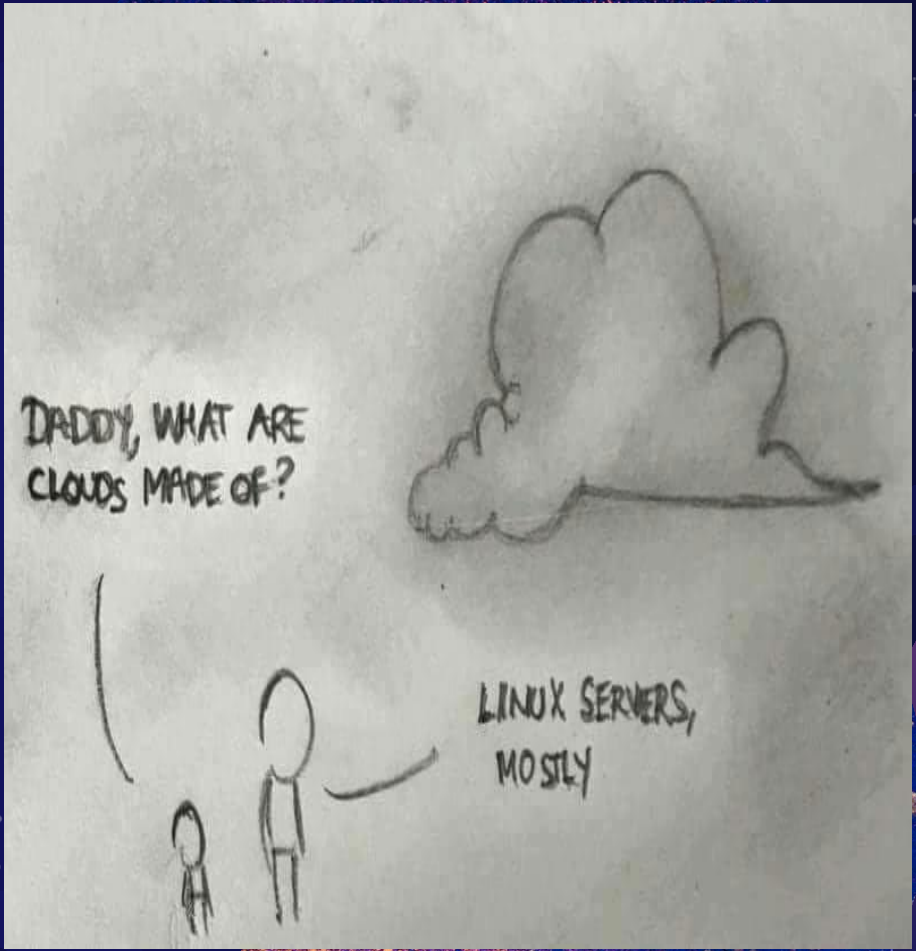
https://www.coreinfrastructure.org/wp-content/uploads/sites/6/2020/02/census_ii_vulnerabilities_in_the_core.pdf

02

A picture always reinforces the concept



Developer	January 2020	Percent	February 2020	Percent	Change
nginx	488,628,547	37.70%	459,966,569	36.48%	-1.22
Apache	310,833,084	23.98%	309,061,300	24.51%	0.53
Microsoft	181,873,181	14.03%	179,225,073	14.21%	0.18
Google	39,081,956	3.02%	40,120,733	3.18%	0.17



# of Active Webservers on the Intertubes – https://news.netcraft.com/archives/category/web-server-survey/

some quick oss stats

# of people contributing

40+Mil Gitlab users
over 10Mil new in 2019 alone

https://octoverse.github.com/

OSS CVE #s?

Searching for “the Linux”
in NVD tells me there were

17,311

OSS CVEs in 2019

WHO IS USING OSS?

2.9+Mil organizations use
public or private git repos

02a

This is a Great Headline:

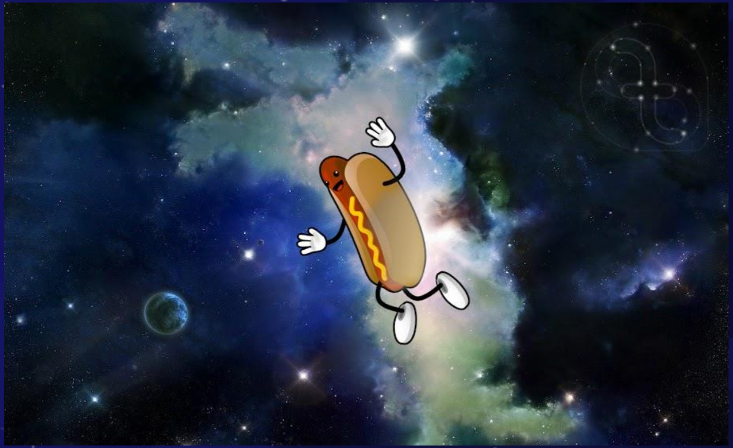
OSS YEAR-IN-REVIEW & TRENDY TRENDS!

our perspective!

Red Hat Inc – a small enterprise software company using an open source development model

- 25+ years in the industry
- Community leadership in
  - Linux Kernel
  - Kubernetes
  - Apache Foundation
  - OpenSSL
  - RDO
  - ...and SO many more

!



Every year we compile a **Risk Report**, which is the source of a lot of the following data point, augmented with community facts

Where You Get Your Open Source MATTERS

Free Fish aren't Free

We've talked about this before, just because the code is free doesn't mean you want it.

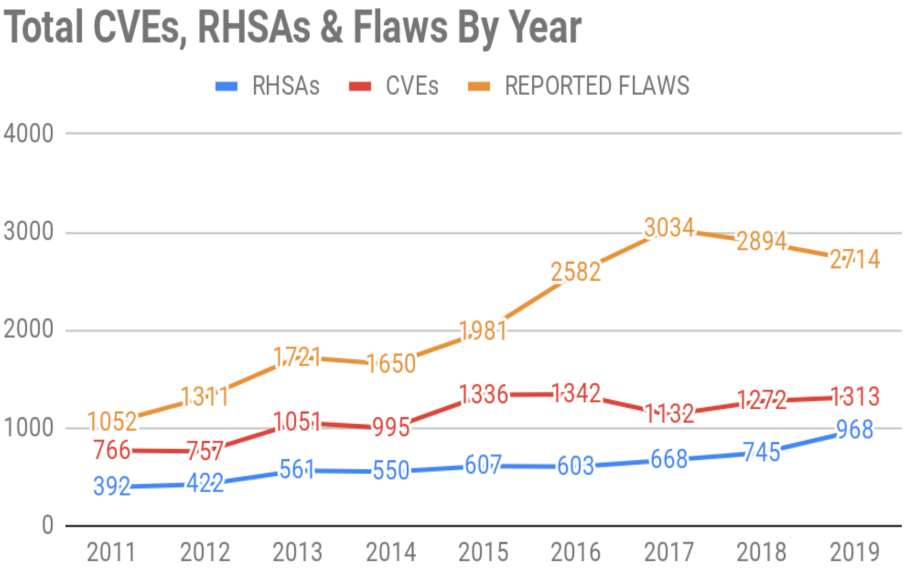
https://www.first.org/resources/papers/hillsboro2019/Free-Fish-Aren-t-Free.pdf

Supply Chain

Your customers are transferring THEIR software risks to YOU, their supplier, and are expecting YOU to conduct reasonable due diligence/management of the bits you give THEM

https://www.linuxfoundation.org/wp-content/uploads/2020/02/oss_supply_chain_security.pdf

Reinforce the concept using graphs and charts!



Flaws reported

Some years are busier than others, but overall our Incoming must sift through A LOT of reports

Advisories issued

This is a result of more products and more longer-life support streams. This is new work for product engineering and our customers to address

CVEs Fixed

Certainly not out busiest year (/me shakes fist at 2016) we fixed more vulnerabilities than the last several years

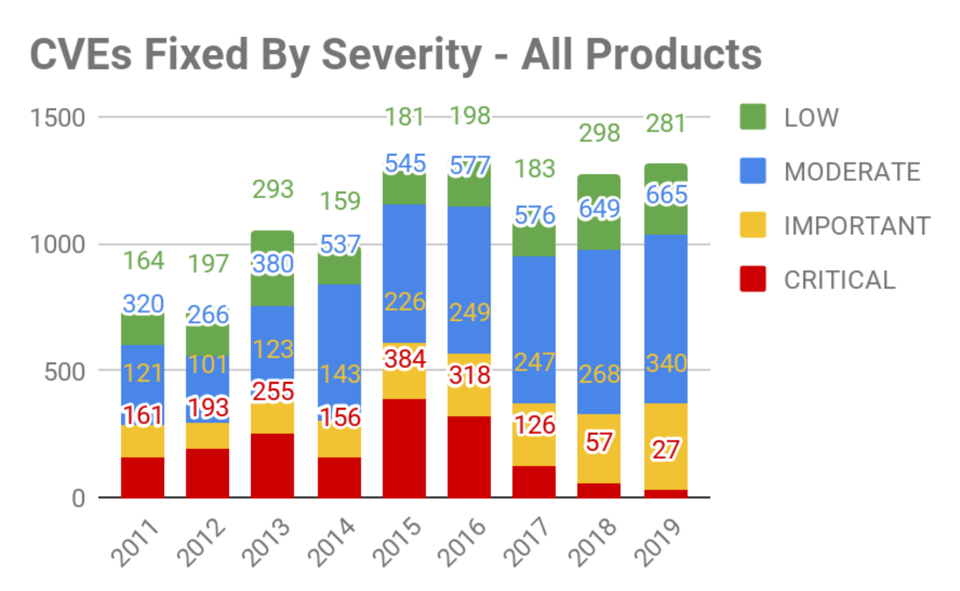
Trend observations

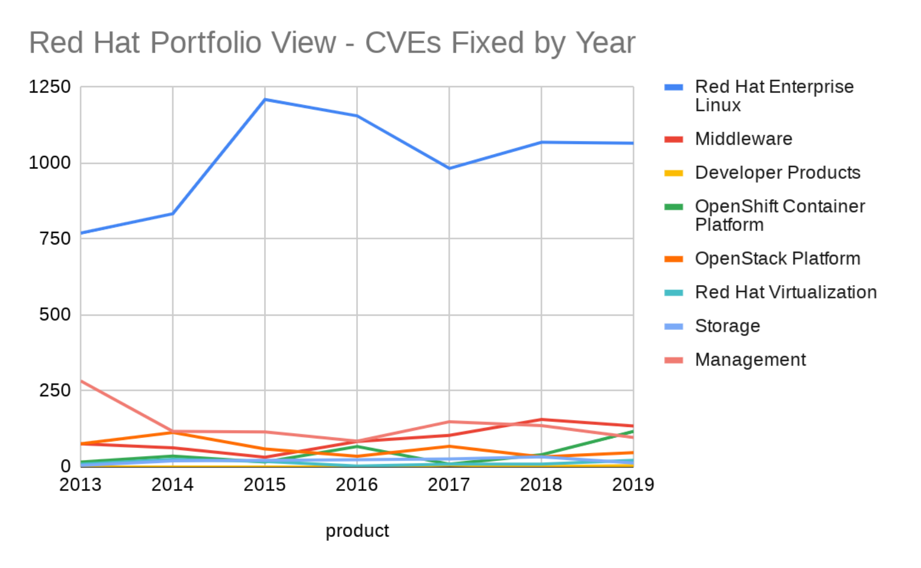
More vulns are found every year, our customers want more patches more quickly to "make the scanner pain go way" <-- more on THIS in a bit!

Think about the Attack Surface you are supporting

Product	# of packages
Red Hat Enterprise Linux 8.1 - default w/GUI	1348 RPMs
Red Hat Enterprise Linux 8.1 minimal	405 RPMs
Red Hat Enterprise Linux 8.1 - full	2321 RPMs [525 (Base OS) + 1796 (AppStream)]
Red Hat Enterprise Linux 7.7 – default	343 RPMs
Red Hat Enterprise Linux 7.7 – full	2319 RPMs
Red Hat OpenStack Platform 15	736 RPMs + underlying OS
Red Hat OpenShift Container Platform 4.2	200 components + underlying OS
Red Hat JBoss Enterprise Application Platform 7.2.4	530 jars + underlying OS

“Fun” Fact - Red Hat Product Security monitors over 450,000 OSS packages/versions that are included in our portfolio





I see VULNERABILITIES

Overall, we're seeing fewer CRITICAL issues, but are slowly being flooded by MODERATES

Component	# of CVE's (this includes multiple affected version numbers of a product)	CWE counts (included if 15+ for top 5)
kernel	216	[illegible] cwe-400(22), cwe-284(20), cwe-416(16)
[illegible]	156	[illegible](24), cwe-843(15)
jackson-databind	[illegible]	cwe-502(93), cwe-502->cwe-200(18)
kernel-rt	112	cwe-200(13), cwe-385->cwe-203(13), cwe-416(13)
mysql:8.0/mysql	95	n/a
rh-mysql80-mysql	95	n/a
java-1.8.0-ibm	69	cwe-20(8)
qemu-kvm-rhev	59	cwe-122(13), cwe-203->cwe-385(24)
qemu-kvm	44	cwe-203->cwe-385(32)
libvirt	39	cwe-203->cwe-385(32)

Uncontrolled Resource Consumption

Since 2019 did not pan out to be the year of the Linux desktop, let's put these 3 packages to the side.

Maybe 2020 will be our year?

Deserialization of Untrusted Data

Nar-nope

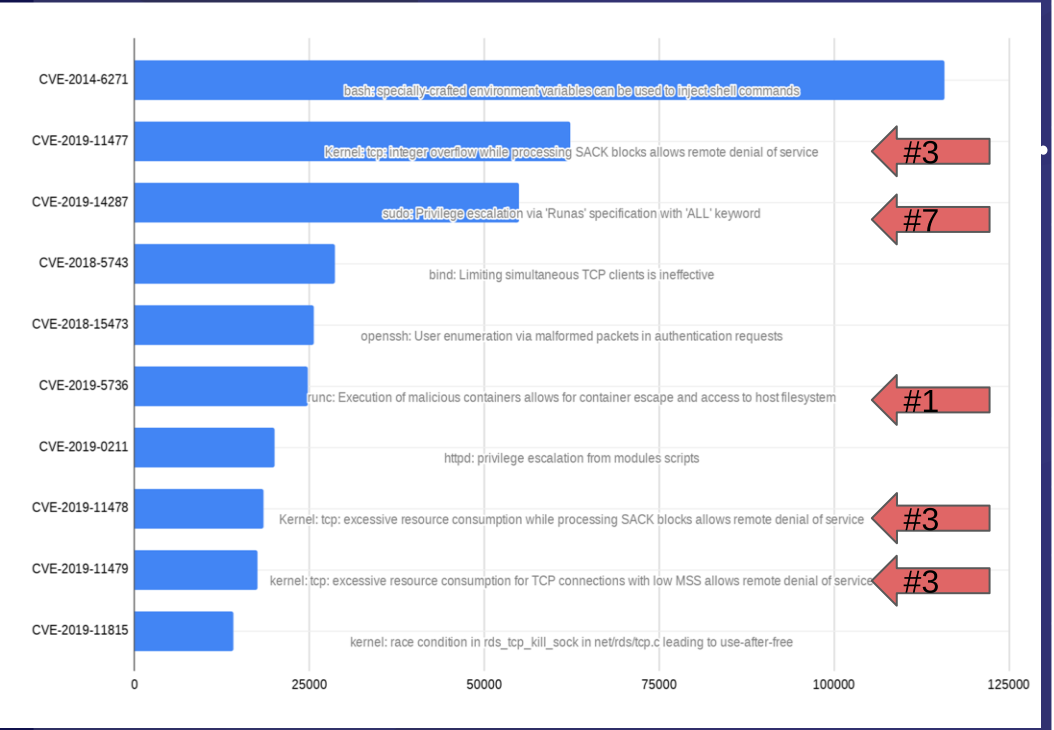
Covert Timing Channel

02B

THIS IS a Great HeaDLINe:

Trendy Trends that are trendily trending!

Interesting Issues of 2019



	CVE	Name	Severity
1	CVE-2019-5763	runc malicious container escape	IMPORTANT
2	CVE-2018-12130, CVE-2018-12126, CVE-2018-12127 & CVE-2019-11091	MDS - Microarchitectural Data Sampling	IMPORTANT / MODERATE
3	CVE-2019-11477, CVE-2019-11478, & CVE-2109-11479	TCP SACK Panic	IMPORTANT / MODERATE
4	CVE-2019-10161, CVE-2019-10166, CVE-2019-10167, & CVE-2019-10168	libvirt privilege escalation	IMPORTANT
5	CVE-2019-1125	Spectre SWAPGS gadget vulnerability	MODERATE
6	CVE-2019-14835	VHOST-NET Guest-to-Host Escape	IMPORTANT
7	CVE-2019-14287	sudo: Privilege escalation via 'Runas'	IMPORTANT
8	CVE-2018-12207	Machine Check Error on Page Size Change	IMPORTANT
9	CVE-2019-11135	Transactional Synchronization Extensions (TSX) Asynchronous Abort	MODERATE
10	CVE-2019-0155 & CVE-2019-0154	i915 Graphic Driver	IMPORTANT / MODERATE

#@$%!

SCANNER.VENDORS--

package version# != RISK

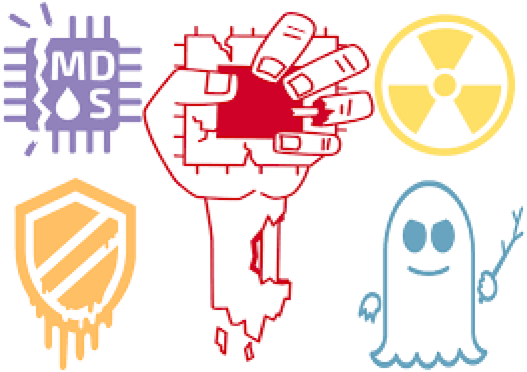
https://www.redhat.com/en/blog/why-cvss-does-not-equal-risk-how-think-about-risk-your-environment

The DEATH of the BRANDED FLAW ?

While I'm not putting out the "Mission Accomplished" banner just yet….

2019 saw a BIG drop in nonsense around branding of flaws, with only a few passing our desks that tried to set the hype to 11.

Our customers were not impressed by the marketing this time around. Ideally this trend continues into 2020 and BEYOND!



NOT ONE CPU FLAW OR BRANDED ISSUE WAS BEHIND ANY REPORTED 2019 BREACHES

Our pals at Verizon s
execs are TWELVE ti
be a target of social a

C-level folks don't have
important, right?

mail is STILL the
or. Ransomware
those campaigns.

MOST SECURITY INCIDENTS OUR CUSTOMERS EXPERIENCE ARE A COMBINATION OF INTENTIONAL OR UNINTENDED HUMAN ERROR, POOR SECURITY HYGIENE, OR LACK OF SECURITY AWARENESS

Cloud is great for
Cool story, bro…i

Attackers are using DevOps practices to scale up/scale down their attacks to be more cost-effective as well as probing this "new datacenter" for open vulnerabilities

https://enterprise.verizon.com/resources/reports/dbir/

AS A DISCIPLINE/INDUSTRY, INFORMATION SECURITY IS FOCUSING ON THE WRONG

Now, a more sobering topic

RIPPED FROM THE HEADLINES!

"According to the Github discussion …. the longtime event-stream developer no longer had time to provide updates. So several months ago, he accepted the help of an unknown developer. The new developer took care to keep the backdoor from being discovered. Besides being gradually implemented in stages, it also narrowly targeted only the Copay wallet app. The malicious code was also hard to spot because the flatmap-stream module was encrypted."

- Ars Technica 11/26/2018

APRIL 2018

webmin - web-based admin tool - unknown attacker changes password_change.cgi - downloaded over 491,000 times

DEC 2018

cloudhopper - supply chain attack targeting HPE & IBM to exploit THEIR customers

NOV 2018

event-stream - popular oss library (over 2mil users)- malicious code inserted targeting Copay bitcoin wallets

KEEPING AN EYE ON THE SUPPLY

TO DATE these attacks seem to be very targeted, most seeking to embed cryptocurrency miners or to redistribute malware to execute 2nd-stage attacks/move laterally post-compromise.

My PERSONAL favourite being DORKBOT, an IRC-based worm that seeks to scrape sensitive info and conduct DDoS attacks IRC.4EVA,YO!

In a 2019 report, Symantec observed supply chain attacks rose 78% in 2018.

I'm "eagerly" waiting for this year's iteration of that research.

https://www.mhlnews.com/global-supply-chain/article/22055712/supply-chain-facing-increased-cyber-attacks
https://www.microsoft.com/security/blog/2019/10/16/guarding-against-supply-chain-attacks-part-1-big-picture/

03

THIS IS a Great HeaDLINe:

Conclusions, Advice, and shoulders to cry upon

WHERE You Get Your Software Matters

What can you do to protect yourself and your customers?

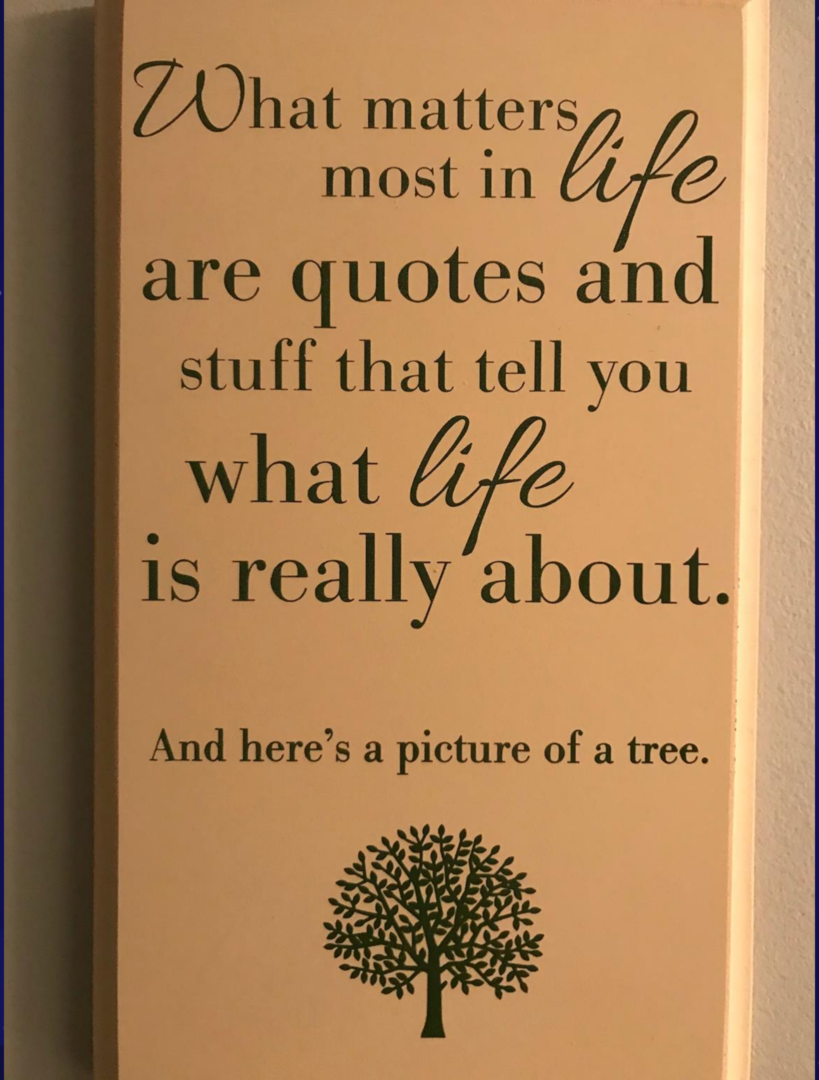
Only download software from KNOWN good sources

Dedicate resources (people, tools, infra) to the projects that matter to you

Conduct your own scans/assessments to ensure code meets your quality standards

Partner with an OSS vendor you can hold accountable

...Enhance your calm



What matters
most in life
are quotes and
stuff that tell you
what life
is really about.

And here's a picture of a tree.

keep breathing, it'll
all be OK

sometimes, reviewing concepts is a GOOD IDea

KNOW THYSELF

If you do not understand what makes up your products, how can you protect them?

OSS COMMUNITIES ARE THRIVING

Dozens of new projects come online daily

SUPPLY CHAIN

YOU get to hold your customers' oss-cyber risk (yay you!). Inspect where your code comes from and how it changes

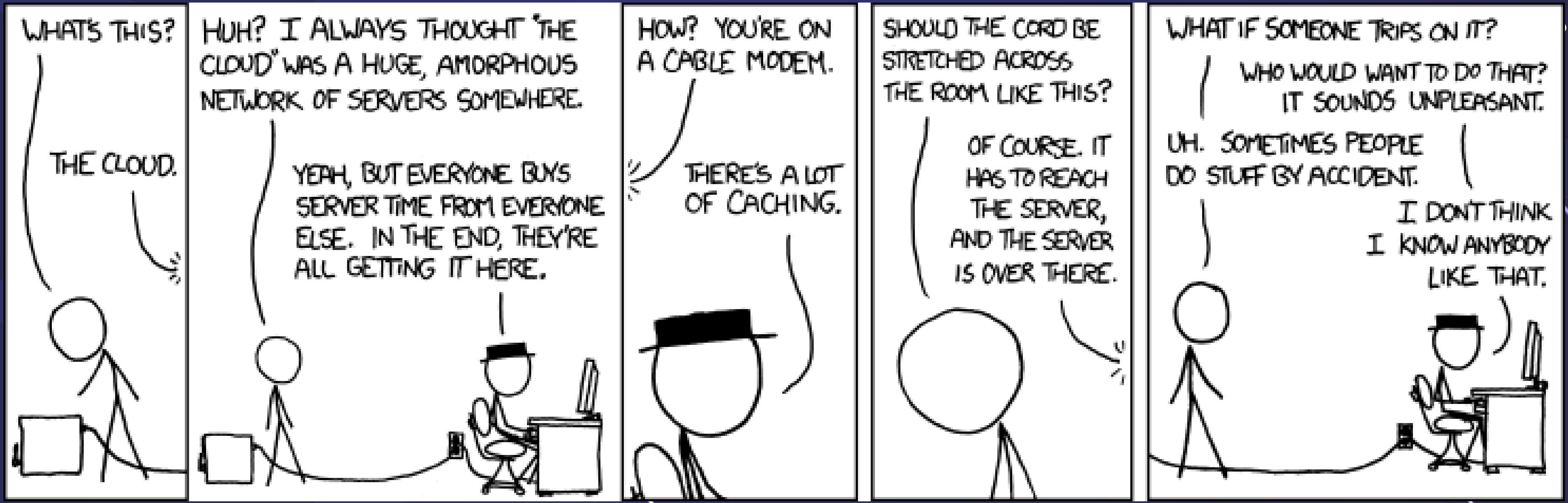
YOU ARE NOT ALONE

Not only are OSS-communities welcoming, so are orgs like FIRST!

THanks!

Does anyone have any questions?

crob_at_redhat_dot_com
@RedHatCRob
the interwebs


WHAT'S THIS?
THE CLOUD.
HUH? I ALWAYS THOUGHT 'THE CLOUD' WAS A HUGE, AMORPHOUS NETWORK OF SERVERS SOMEWHERE.
YEAH, BUT EVERYONE BUYS SERVER TIME FROM EVERYONE ELSE. IN THE END, THEY'RE ALL GETTING IT HERE.
HOW? YOU'RE ON A CABLE MODEM.
THERE'S A LOT OF CACHING.
SHOULD THE CORD BE STRETCHED ACROSS THE ROOM LIKE THIS?
OF COURSE. IT HAS TO REACH THE SERVER, AND THE SERVER IS OVER THERE.
WHAT IF SOMEONE TRIPS ON IT?
WHO WOULD WANT TO DO THAT? IT SOUNDS UNPLEASANT.
UH. SOMETIMES PEOPLE DO STUFF BY ACCIDENT.
I DON'T THINK I KNOW ANYBODY LIKE THAT.

CREDITS

This is where you give credit to the ones who are part of this project.

Did you like the resources on this template? Get them for free at our other websites.

- Presentation template by Slidesgo
- Icons by Flaticon
- Images & infographics by Freepik
- Author introduction slide photo created by Freepik
- Text & Image slide photo created by Freepik.com
- Big image slide photo created by Freepik.com