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>
<thead>
<tr>
<th>01</th>
<th><strong>INTRODUCTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Why OSS is important</td>
</tr>
<tr>
<td>02</td>
<td><strong>PRESENTATION</strong></td>
</tr>
<tr>
<td></td>
<td>The stuff about the title that draw you to sit here and listen</td>
</tr>
<tr>
<td>03</td>
<td><strong>CONCLUSION</strong></td>
</tr>
<tr>
<td></td>
<td>Reflections on the amazing revelations you have witnessed during the hour</td>
</tr>
</tbody>
</table>
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

A picture always reinforces the concept.
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!
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.


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.

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

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th># OF PACKAGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux 8.1 - default w/GUI</td>
<td>1348 RPMs</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 8.1 minimal</td>
<td>405 RPMs</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 8.1 - full</td>
<td>2321 RPMs [525 (Base OS) + 1796 (AppStream)]</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 7.7 - default</td>
<td>343 RPMs</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 7.7 - full</td>
<td>2319 RPMs</td>
</tr>
<tr>
<td>Red Hat OpenStack Platform 15</td>
<td>736 RPMs + underlying OS</td>
</tr>
<tr>
<td>Red Hat OpenShift Container Platform 4.2</td>
<td>200 components + underlying OS</td>
</tr>
<tr>
<td>Red Hat JBoss Enterprise Application Platform 7.2.4</td>
<td>530 jars + underlying OS</td>
</tr>
</tbody>
</table>

“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.
<table>
<thead>
<tr>
<th>Component</th>
<th># of CVE's (this includes multiple affected version numbers of a product)</th>
<th>CWE counts (included if 15+ for top 5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>kernel</td>
<td>216</td>
<td>cwe-200(19), cwe-203-&gt;cwe-385(47), cwe-400(22), cwe-416(16)</td>
</tr>
<tr>
<td>thunderbird</td>
<td>156</td>
<td>cwe-120(24), cwe-416(27), cwe-829(24), cwe-843(15)</td>
</tr>
<tr>
<td>firefox</td>
<td>152</td>
<td>cwe-120(25), cwe-416(27), cwe-829(24), cwe-843(16)</td>
</tr>
<tr>
<td>chromium-browser</td>
<td>131</td>
<td>cwe-416(2), cwe-20(1), cwe-125(1)</td>
</tr>
<tr>
<td>jackson-databind</td>
<td>123</td>
<td>cwe-502(93), cwe-502-&gt;cwe-200(18)</td>
</tr>
<tr>
<td>kernel-rt</td>
<td>112</td>
<td>cwe-200(13), cwe-385-&gt;cwe-203(13), cwe-416(13)</td>
</tr>
<tr>
<td>mysql:8.0/mysql</td>
<td>95</td>
<td>n/a</td>
</tr>
<tr>
<td>rh-mysql80-mysql</td>
<td>95</td>
<td>n/a</td>
</tr>
<tr>
<td>java-1.8.0-ibm</td>
<td>69</td>
<td>cwe-20(8)</td>
</tr>
<tr>
<td>qemu-kvm-rhev</td>
<td>59</td>
<td>cwe-122(13), cwe-203-&gt;cwe-385(24)</td>
</tr>
<tr>
<td>qemu-kvm</td>
<td>44</td>
<td>cwe-203-&gt;cwe-385(32)</td>
</tr>
<tr>
<td>libvirt</td>
<td>39</td>
<td>cwe-203-&gt;cwe-385(32)</td>
</tr>
</tbody>
</table>

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?*
Trendy Trends that are trendily trending!
## Interesting Issues of 2019

<table>
<thead>
<tr>
<th>#</th>
<th>CVE</th>
<th>Name</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CVE-2019-5763</td>
<td>runc malicious container escape</td>
<td>IMPORTANT</td>
</tr>
<tr>
<td>5</td>
<td>CVE-2019-1125</td>
<td>Spectre SWAPGS gadget vulnerability</td>
<td>MODERATE</td>
</tr>
<tr>
<td>6</td>
<td>CVE-2019-14835</td>
<td>VHOST-NET Guest-to-Host Escape</td>
<td>IMPORTANT</td>
</tr>
<tr>
<td>7</td>
<td>CVE-2019-14287</td>
<td>sudo: Privilege escalation via 'Runas'</td>
<td>IMPORTANT</td>
</tr>
<tr>
<td>8</td>
<td>CVE-2018-12207</td>
<td>Machine Check Error on Page Size Change</td>
<td>IMPORTANT</td>
</tr>
<tr>
<td>9</td>
<td>CVE-2019-11135</td>
<td>Transactional Synchronization Extensions (TSX) Asynchronous Abort</td>
<td>MODERATE</td>
</tr>
</tbody>
</table>
#@$%!  

SCANNER.VENDORS--

package version# != RISK

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 state the C-level execs are TWELVE times more likely to be a target of social attacks.

C-level folks don’t have access to anything important, right?

Cloud is great for yours and your customers’ businesses...

Cool story, bro...it’s great for the attackers too!

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

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

Malware delivered via e-mail is STILL the most popular attack vector. Ransomware was involved in ~ 24% of those campaigns.

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

https://enterprise.verizon.com/resources/reports/dbir/
Now, a more sobering topic

I don't know how to put this

But I'm kind of a big deal
“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
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.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
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
WHY'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.
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