anchore

The Lessons of Log4shell

Preparing for the Next Zero-Day

Hello World

Paul Novarese

Principal Solutions Architect

Anchore, Inc.

github.com/pvnovarese

Fediverse: @pvn@mas.to

Agenda

01 When

02 What

03 Who

04 How

anchore


log5j

anchore

Lesson 1: When


Fukishima Daiichi
Incident: 2011
Cleanup: at LEAST thirty years


Chernobyl
Incident: 1986
Cleanup: at LEAST until 2065

Home / Risk Management

With 40% of Log4j Downloads Still Vulnerable, Security Retrofitting Needs to B… Full-Time Job

Log4j flaw: Why it will still be causing problems a decade from now

Log4Shell ain't over until it's over, warns the US review board tasked with investigating the critical Apache Log4J flaw known as Log4Shell.

Written by Liam Tung, Contributing Writer on July 15, 2022

Mark Chmarny (He/Him) • Following
Product, Infra & DevEx at Cruise
4mo •

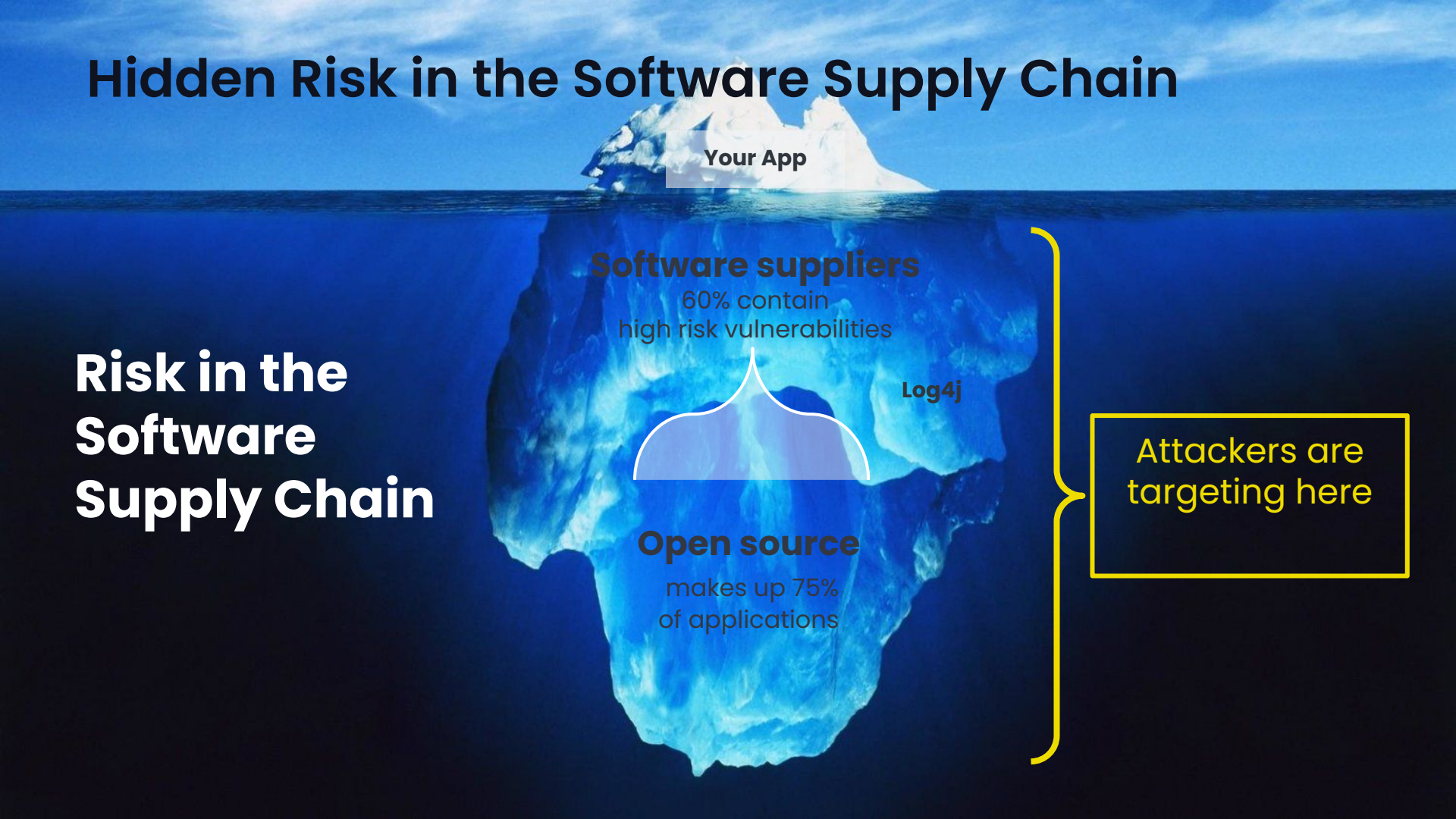
29% of Log4j consumption worldwide STILL uses versions that are known to be vulnerable (source: Sonatype)


WE ARE NEVER EVER EVER
GETTING RID OF LOG4SHELL
quickmeme.com

anchore

Lesson 2: What

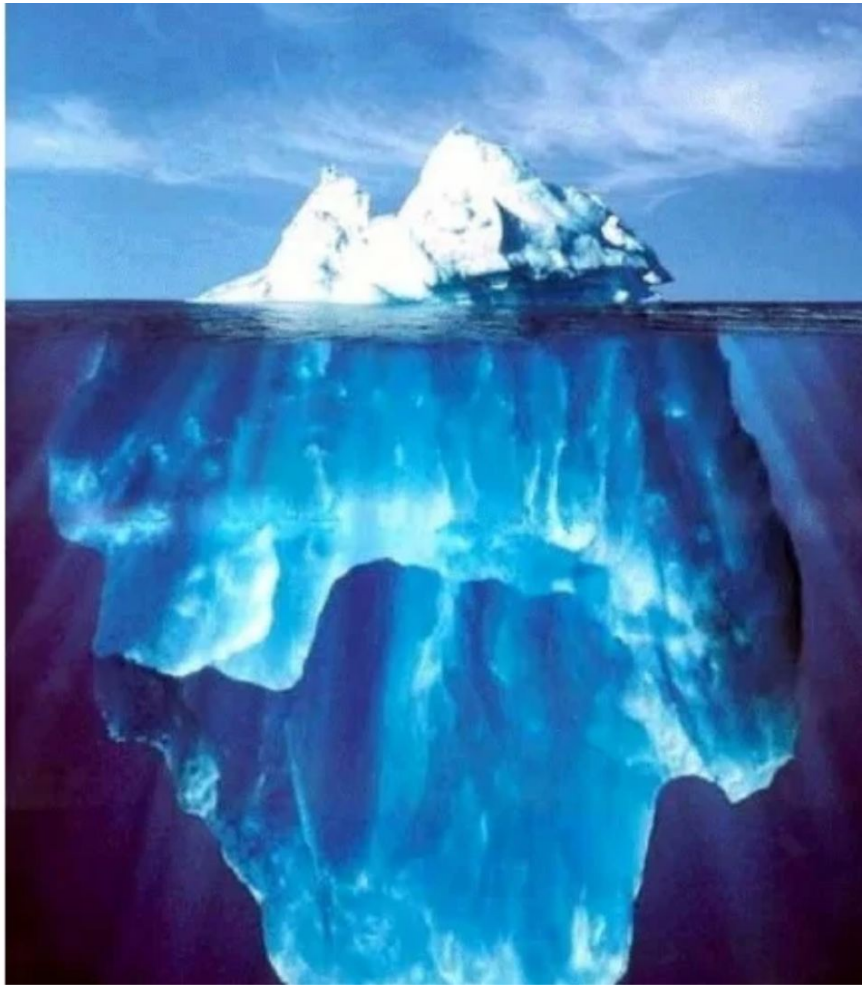
Hidden Risk in the Software Supply Chain

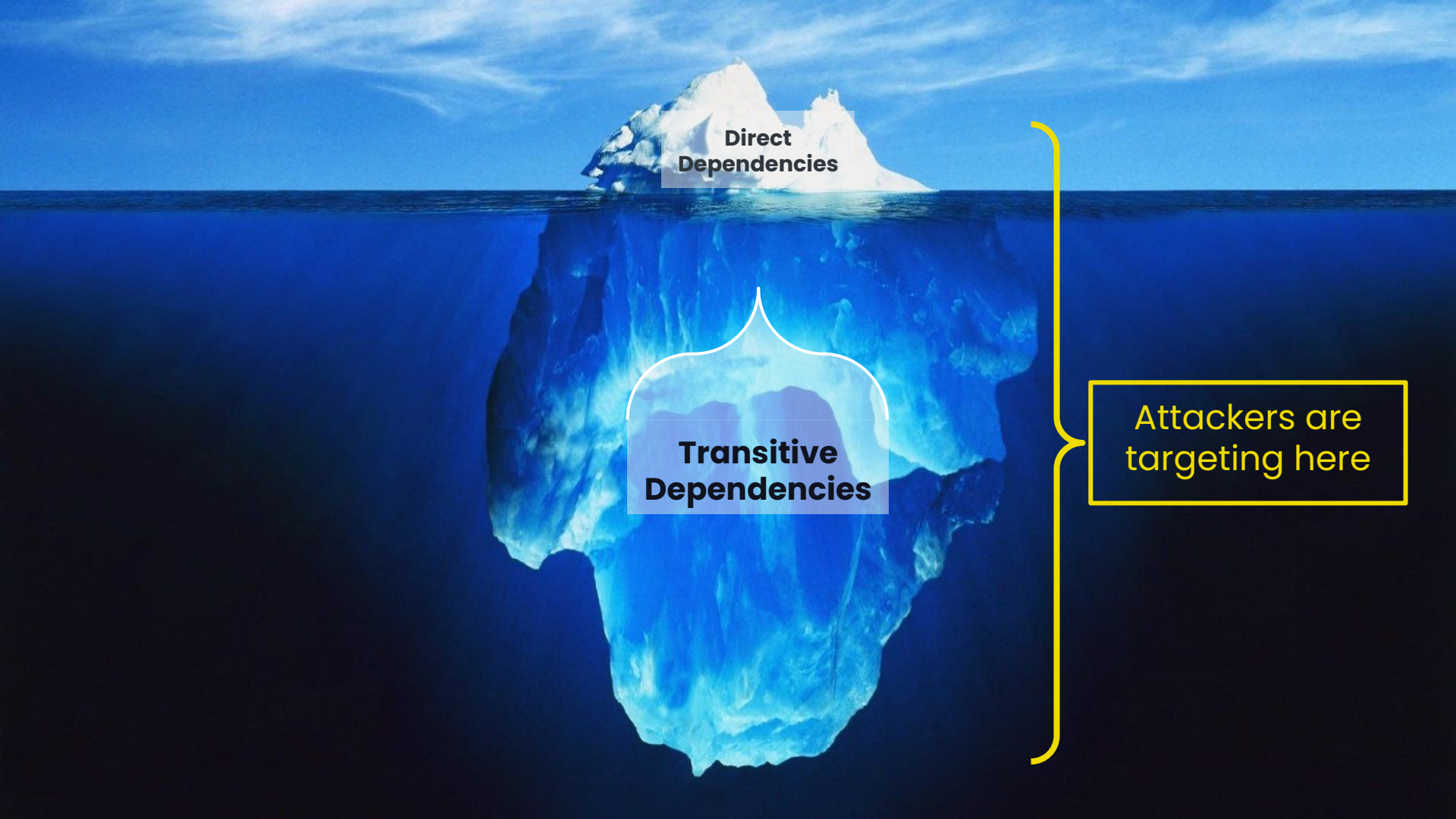


Risk in the Software Supply Chain

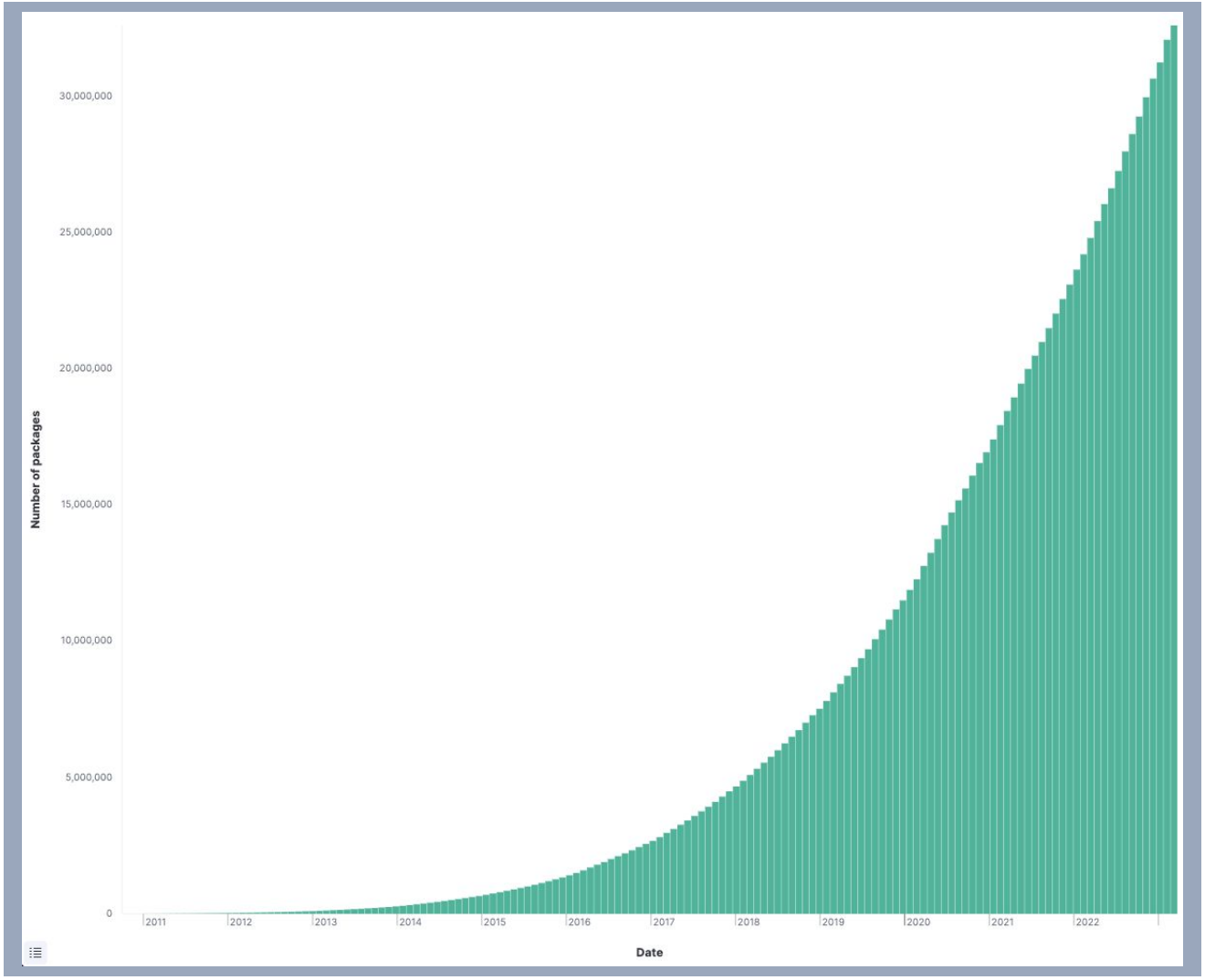
Free is Just the Tip of the Iceberg: Open Source Library System Software

Lori Bowen Ayre
lori.ayre@galecia.com
METRO Webinar
October 6, 2009

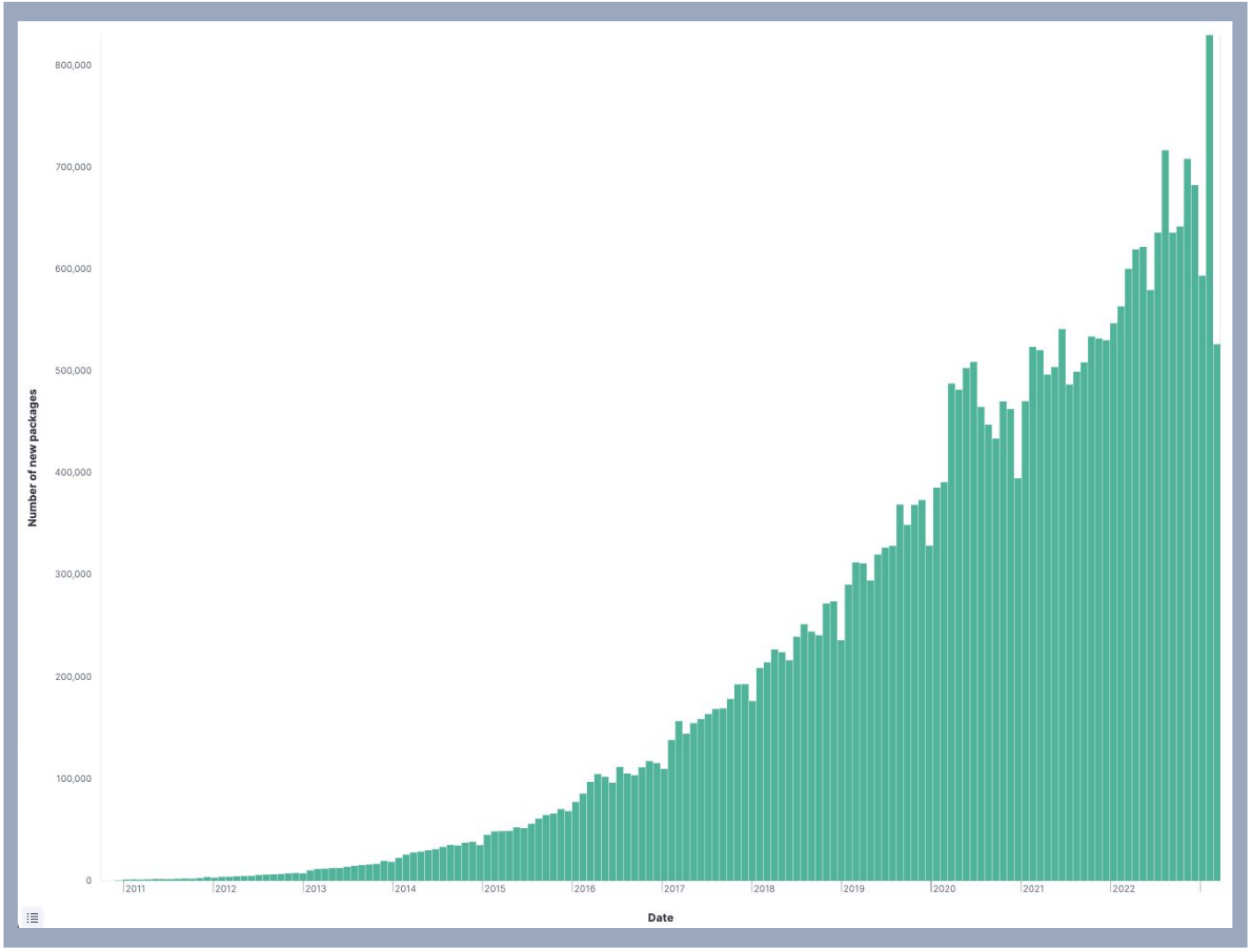



Direct
Dependencies
Transitive
Dependencies
Attackers are
targeting here

Number of
NPM packages

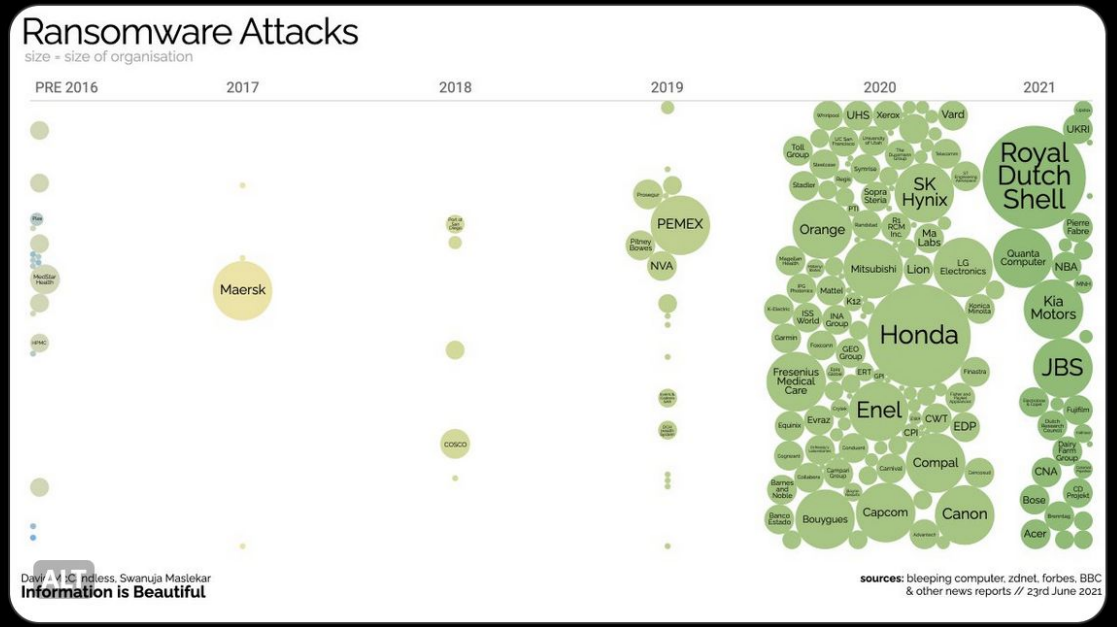


Number of
NEW packages



Information is Beautiful
@infobeautiful

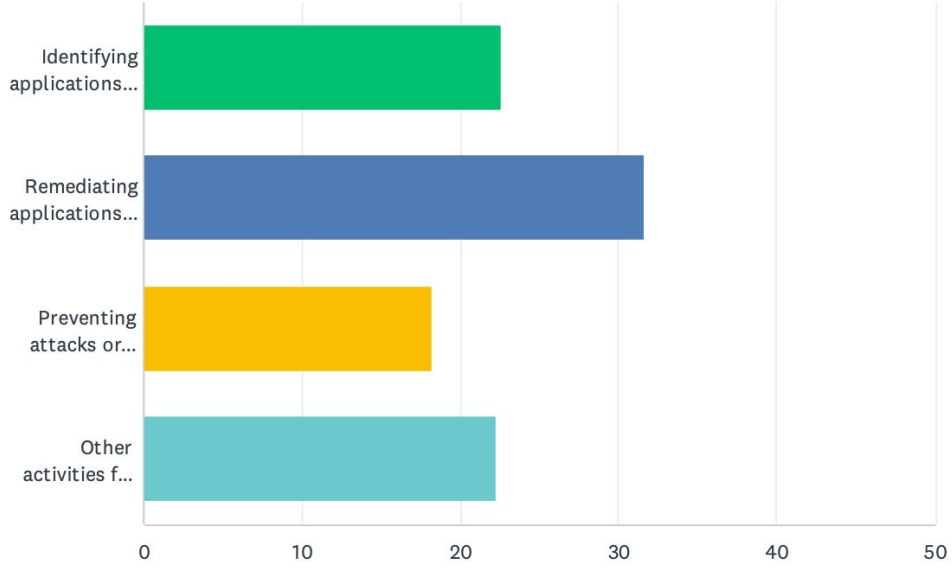
Are #Ransomware attacks increasing? I think #Ransomware attacks are increasing...
interactive: bit.ly/3h1lYPs



11:33 AM · Jun 23, 2021

Q12 Estimate how many hours you personally have spent to date on each of the following activities.

Answered: 195 Skipped: 15



anchore

Lesson 3: Who

daniel:// stenberg://
@bagder

If you are a multi billion dollar company and are concerned about log4j, why not just email OSS authors you never paid anything and demand a response for free within 24 hours with lots of info? (company name redacted for *my* peace of mind)

Dear Haxx Team Partner,

You are receiving this message because [redacted] uses a product you developed. We request you review and respond within 24 hours of receiving this email. If you are not the right person, please forward this message to the appropriate contact.

As you may already be aware, a newly discovered zero-day vulnerability is currently impacting Java logging library Apache Log4j globally, potentially allowing attackers to gain full control of affected servers.

The security and protection of our customers' confidential information is our top priority. As a key partner in serving our customers, we need to understand your risk and mitigation plans for this vulnerability.

Please respond to the following questions using the template provided below.

Stop thinking about open source like a vendor

This

Not this

Number of Maintainers

anchore

Lesson 3: How

Paul Novarese (He/Him) • You
Software Supply Chain Security at Anchore
1yr • Edited •

The #log4j debacle is going to have ramifications far beyond the vulnerability itself. There has been a lot of inertia in how issues are evaluated and classified, how information about those issues is disseminated, and how organizations respond to them, and #log4shell has exposed a lot of these problems. This will be a catalyst for a lot of changes that are way overdue.

April King
@CubicleApril

The fact that there are almost 10,000 CVEs with the same CVSS score as the Log4j vulnerability suggests to me that maybe the scale should be logarithmic.

6:26 PM · Dec 11, 2021 · Twitter for iPhone

71 Retweets **6** Quote Tweets **736** Likes

CVE-2020-19909

On August 25 2023, we got an email to the curl-library mailing list from Samuel Henrique that informed us that "someone" had recently created a CVE, a security vulnerability identification number and report really, for a curl problem.

```
I wanted to let you know that there's a recent
curl CVE published and it doesn't look like it
was acknowledged by the curl authors since it's
not mentioned in the curl website: CVE-2020-19909
```

We can't tell who filed it. We just know that it is now there.

September 4, 2023 – September 11, 2023

Period: 1 week

Overview

20 Active pull requests

13 Active issues

16	4	6	7
Merged pull requests	Open pull requests	Closed issues	New issues

Excluding merges, **9 authors** have pushed **16 commits** to main and **21 commits** to all branches. On main, **20 files** have changed and there have been **240 additions** and **124 deletions**.

1 Release published by **1** person

v0.90.0
published 3 hours ago

16 Pull requests merged by **7** people

fix the help output of power-user
#2113 merged 8 hours ago

anchore

Recap, Notes, &c.

Recap

- Log4Shell is radioactive and immortal
- How software gets made has changed
- We don’t know what’s in our software
- We don’t know who is supplying it
- We have to change how we evaluate it
- GitHub is uniquely positioned
- Think about risk in the general case

anchore

Q&A

Download Syft

https://github.com/anchore/syft

Download Grype

https://github.com/anchore/grype

Let us know if you like it by giving us a star on GitHub

Get an invite to our open source community Slack at
https://anchore.com/slack/

These slides and lab examples archived here:

https://github.com/pvnovarese/2023-09-lessons-of-log4shell

Footnotes

Slide 6 (Log4Shell will still be causing problems a decade from now):
https://www.zdnet.com/article/log4j-flaw-why-it-will-still-be-causing-problems-a-decade-from-now/

Slide 6 (40% of Log4j downloads still vulnerable):
https://securityintelligence.com/articles/log4j-downloads-vulnerable/

Slide 10 (possible origin of the iceberg):
https://www.slideshare.net/loriayre/open-source-library-system-software-free-is-just-the-tip-of-the-iceberg

Slides 12,13, 22 (Open Source is Bigger Than You Can Imagine):
https://anchore.com/blog/open-source-is-bigger-than-you-imagine/

Slide 14 (log4j survey etc):
https://anchore.com/log4j/

Slide 18:
https://twitter.com/CubicleApril/status/1469825942684160004
https://www.linkedin.com/posts/novarese_log4j-log4shell-activity-6876206319238463488-8bEA

Slide 26:
https://twitter.com/bagder/status/1484672924036616195
https://lists.haxx.se/pipermail/daniel/2023-September/000032.html

anchore

Reading List

GitHub Advisory Database:
https://github.com/advisories

GitHub Insights:
https://docs.github.com/en/issues/planning-and-tracking-with-projects/viewing-insights-from-your-project/about-insights-for-projects

CVEs CWEs CVSS and It's Discontents
https://www.linkedin.com/pulse/cves-cwes-cvss-its-discontents-sherif-mansour

Open Source Security Podcast Episode 392 – Curl and the calamity of CVE
https://opensourcesecurity.io/2023/09/10/episode-392-curl-and-the-calamity-of-cve/

I am not a Supplier:
https://www.softwaremaxims.com/blog/not-a-supplier
https://opensourcesecuritypodcast.libsyn.com/episode-365-i-am-not-your-supplier-with-thomas-depierre

Shedding Light on CVSS Scoring Inconsistencies
https://arxiv.org/abs/2308.15259

My previous DevOpsDays 2022 talk (Learn From Log4Shell):
https://www.youtube.com/watch?v=PlNtIL_oN0k
https://github.com/pvnovarese/2022-devopsdays

Probably Don't Rely on EPSS Yet
https://insights.sei.cmu.edu/blog/probably-dont-rely-on-epss-yet/

CVE-2020-19909 is everything that is wrong with CVEs
https://daniel.haxx.se/blog/2023/08/26/cve-2020-19909-is-everything-that-is-wrong-with-cves/

CISA Known Exploited Vulnerability Catalog
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Exploit Prediction Scoring System
https://www.first.org/epss/

Do SBOMS Need VEX?
https://www.linkedin.com/posts/aph10_sbom-softwaresupplychainsecurity-vex-activity-7108017924384137216-VARV/

Log4Shell Reading List

Dealing with log4shell (detection, mitigation, workarounds):
https://cloudsecurityalliance.org/blog/2021/12/14/dealing-with-log4shell-aka-cve-2021-44228-aka-the-log4j-version-2/

Keeping up with log4shell (post mortem)
https://cloudsecurityalliance.org/blog/2021/12/16/keeping-up-with-log4shell-aka-cve-2021-44228-aka-the-log4j-version-2/

Mysterious tweet hinting at the exploit:
https://twitter.com/sirifu4k1/status/1468951859381485573

Another mysterious tweet:
https://twitter.com/CattusGlavo/status/1469010118163374089

“THE” pull request:
https://github.com/apache/logging-log4j2/pull/608

Cloudflare digs for evidence of pre-disclosure exploits in the wild:
https://twitter.com/eastdakota/status/1469800951351427073

anchore

Appendix A

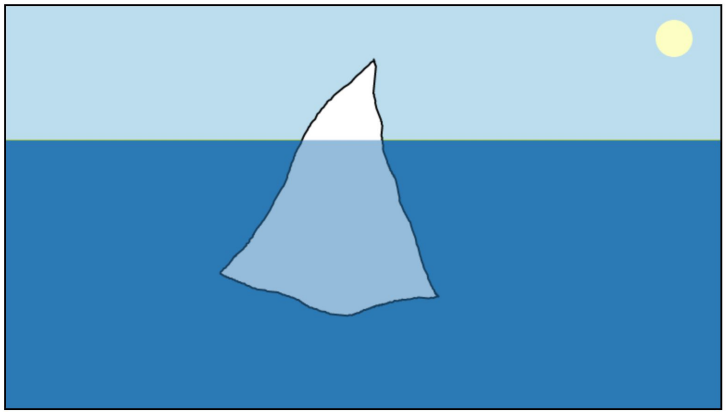
Additional Bonus Slides

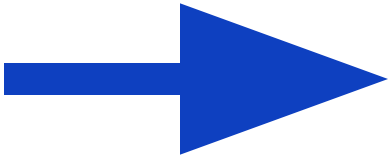
Quick Aside

Iceberger

Draw an iceberg and see how it will float.

(Inspired by a tweet by @GlacialMeg)

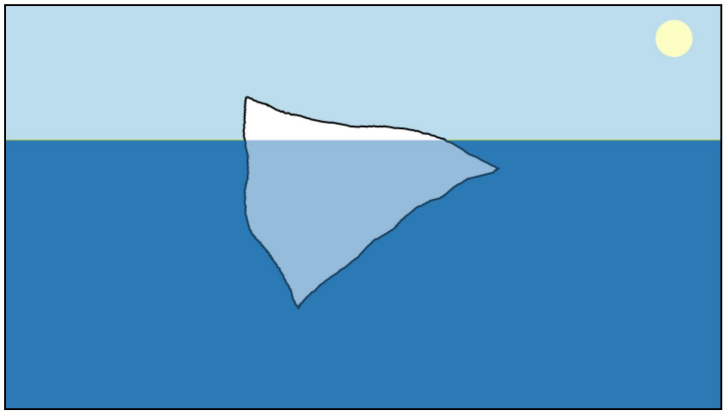




Iceberger

Draw an iceberg and see how it will float.

(Inspired by a tweet by @GlacialMeg)




Today I Fucked Up... (She/Her)
@K_LDivergence
I don't know anything about this
This is beyond the scope of this paper
made with mematic
6:06 PM · Dec 10, 2020