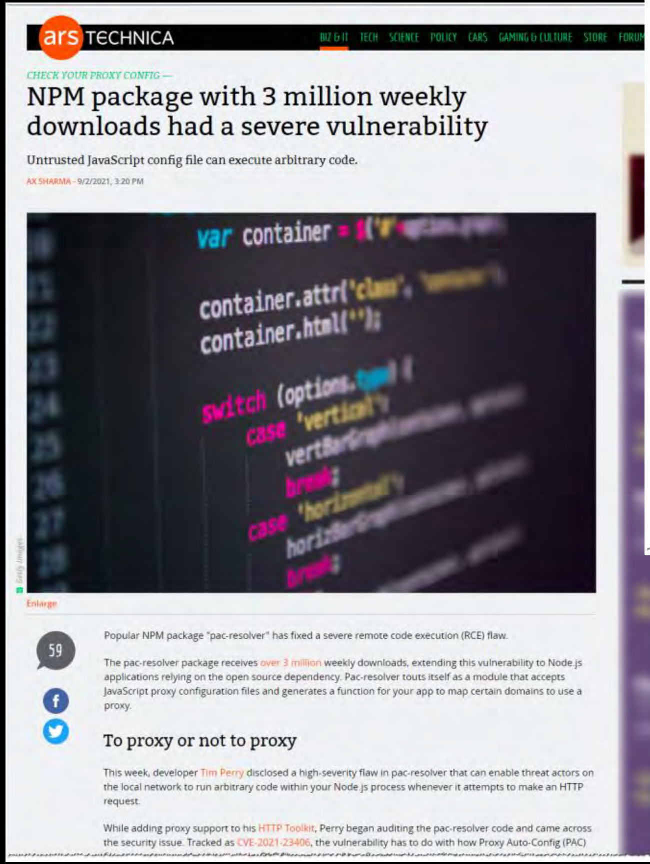
Is Technical Debt the right metaphor for Continuous Update?

Giulio Vian

December 1st, 2023

It happens



CHECK YOUR PROXY CONFIG —

NPM package with 3 million weekly downloads had a severe vulnerability

Untrusted JavaScript config file can execute arbitrary code.

AX SHARMA - 9/2/2021, 3:20 PM

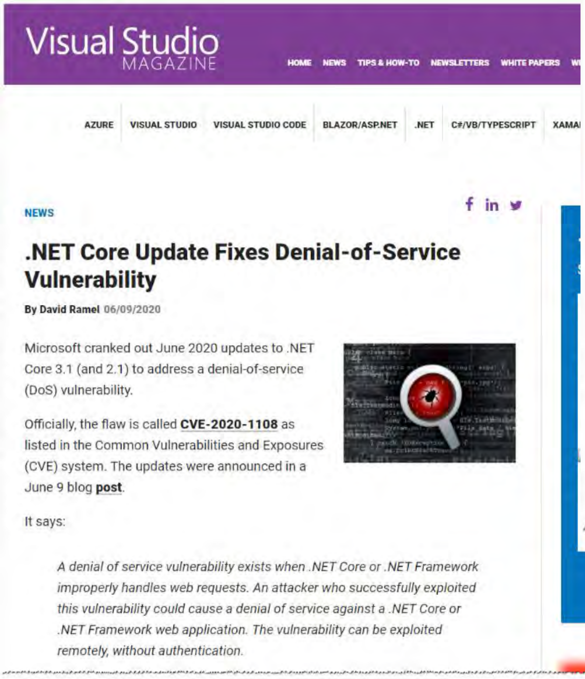
Popular NPM package "pac-resolver" has fixed a severe remote code execution (RCE) flaw.

The pac-resolver package receives over 3 million weekly downloads, extending this vulnerability to Node.js applications relying on the open source dependency. Pac-resolver touts itself as a module that accepts JavaScript proxy configuration files and generates a function for your app to map certain domains to use a proxy.

To proxy or not to proxy

This week, developer Tim Perry disclosed a high-severity flaw in pac-resolver that can enable threat actors on the local network to run arbitrary code within your Node.js process whenever it attempts to make an HTTP request.

While adding proxy support to his HTTP Toolkit, Perry began auditing the pac-resolver code and came across the security issue. Tracked as CVE-2021-23406, the vulnerability has to do with how Proxy Auto-Config (PAC)



NEWS

.NET Core Update Fixes Denial-of-Service Vulnerability

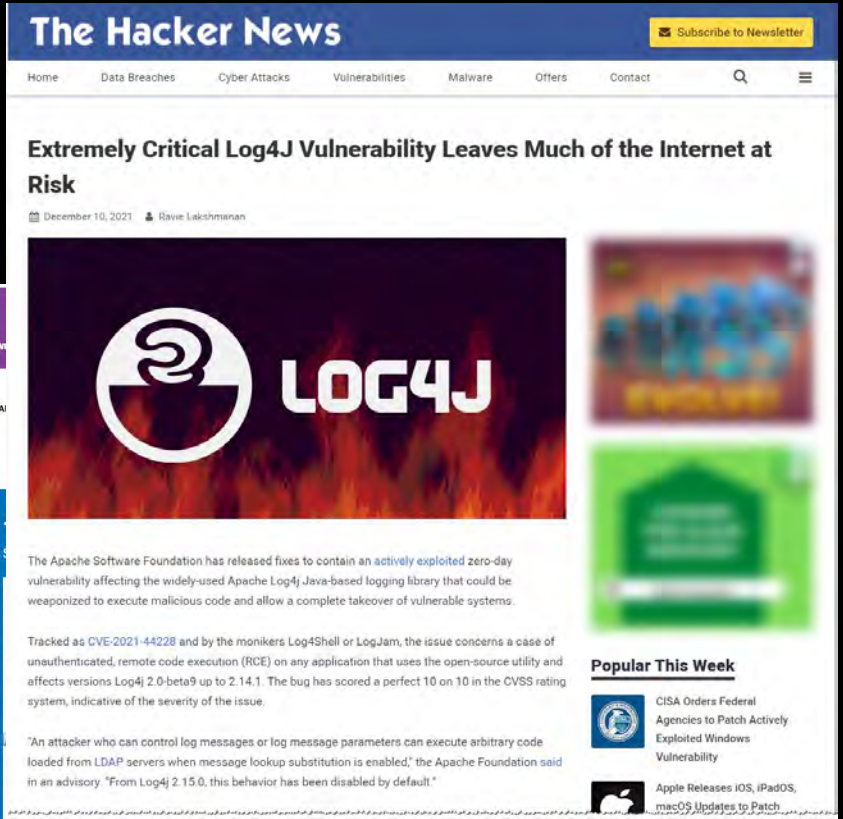
By David Ramel 06/09/2020

Microsoft cranked out June 2020 updates to .NET Core 3.1 (and 2.1) to address a denial-of-service (DoS) vulnerability.

Officially, the flaw is called **CVE-2020-1108** as listed in the Common Vulnerabilities and Exposures (CVE) system. The updates were announced in a June 9 blog **post**.

It says:

> *A denial of service vulnerability exists when .NET Core or .NET Framework improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against a .NET Core or .NET Framework web application. The vulnerability can be exploited remotely, without authentication.*



Extremely Critical Log4J Vulnerability Leaves Much of the Internet at Risk

December 10, 2021 Ravie Lakshmanan

The Apache Software Foundation has released fixes to contain an actively exploited zero-day vulnerability affecting the widely-used Apache Log4j Java-based logging library that could be weaponized to execute malicious code and allow a complete takeover of vulnerable systems.

Tracked as CVE-2021-44228 and by the monikers Log4Shell or LogJam, the issue concerns a case of unauthenticated, remote code execution (RCE) on any application that uses the open-source utility and affects versions Log4j 2.0-beta9 up to 2.14.1. The bug has scored a perfect 10 on 10 in the CVSS rating system, indicative of the severity of the issue.

"An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled," the Apache Foundation said in an advisory. "From Log4j 2.15.0, this behavior has been disabled by default."

Popular This Week

- CISA Orders Federal Agencies to Patch Actively Exploited Windows Vulnerability
- Apple Releases iOS, iPadOS, macOS Updates to Patch

Is it Technical Debt?

Image source: Max Pixel

Agenda

How often do I need to update?

Is it Technical Debt?

What is Continuous Update?

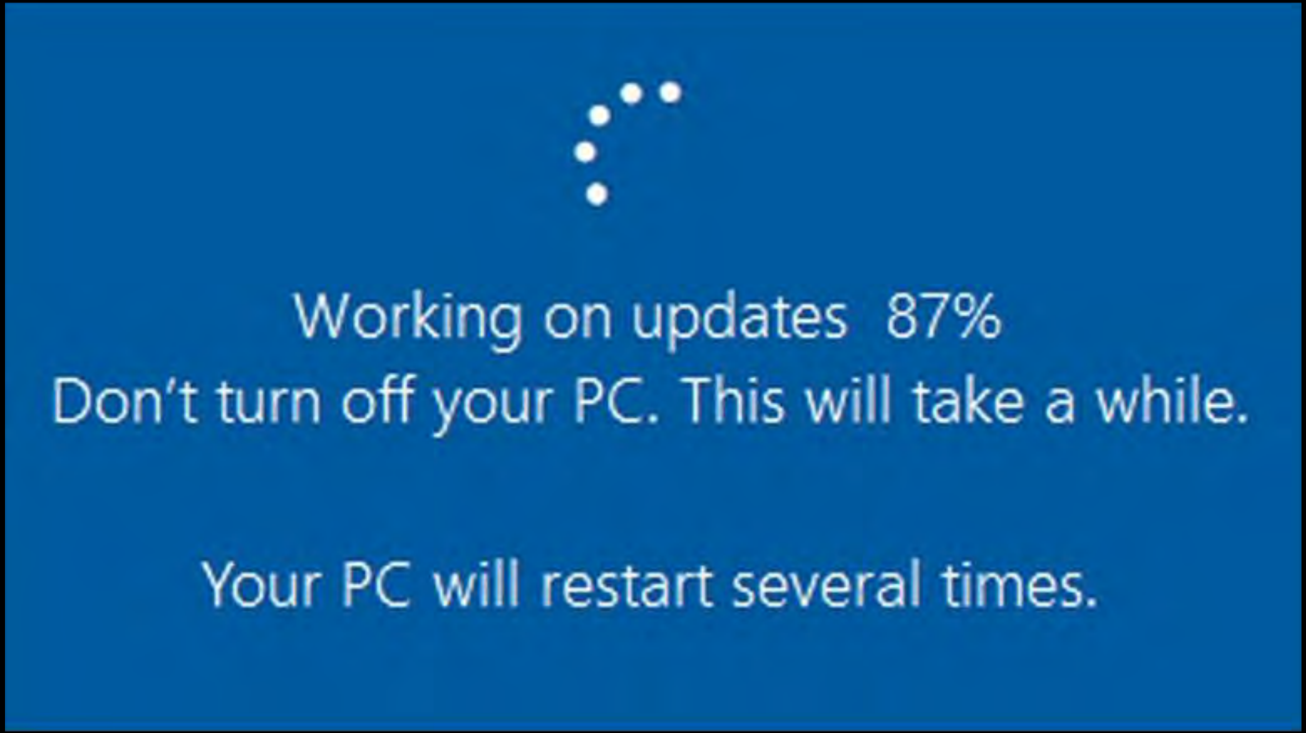
How often do I need to update?

Update what?

Operating System patches

Application stack patches

Libraries updates and patches



Working on updates 87%
Don't turn off your PC. This will take a while.

Your PC will restart several times.

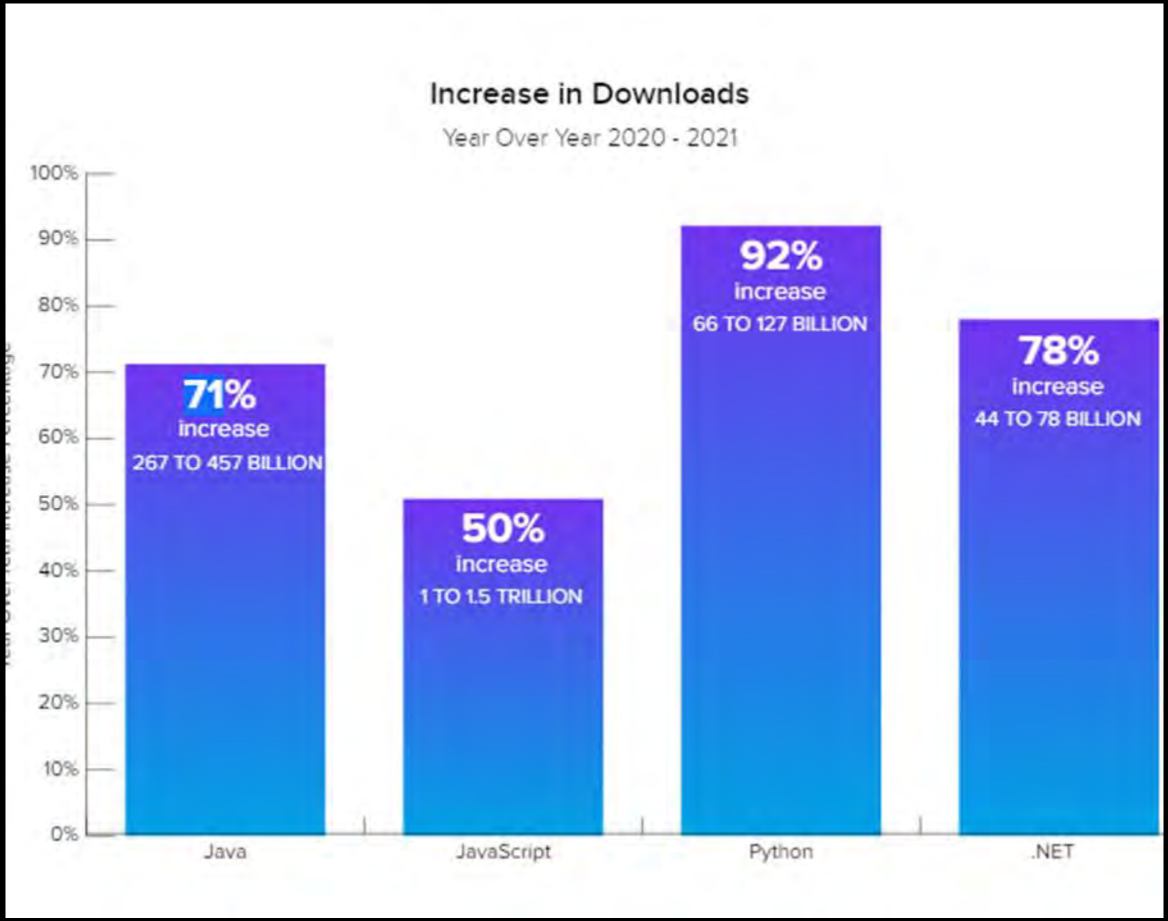
Operating Systems and Images

Platform	Released every	Patched every (avg.)
Alpine	6 months	52.2 days (7.5 weeks)
Ubuntu	2 years (LTS) 6 months	21.8 days
Amazon Linux	2 years (LTS) 3 months	21.7 days
Windows Server	3 years 6 months	monthly Patch Tuesday

Application Platforms

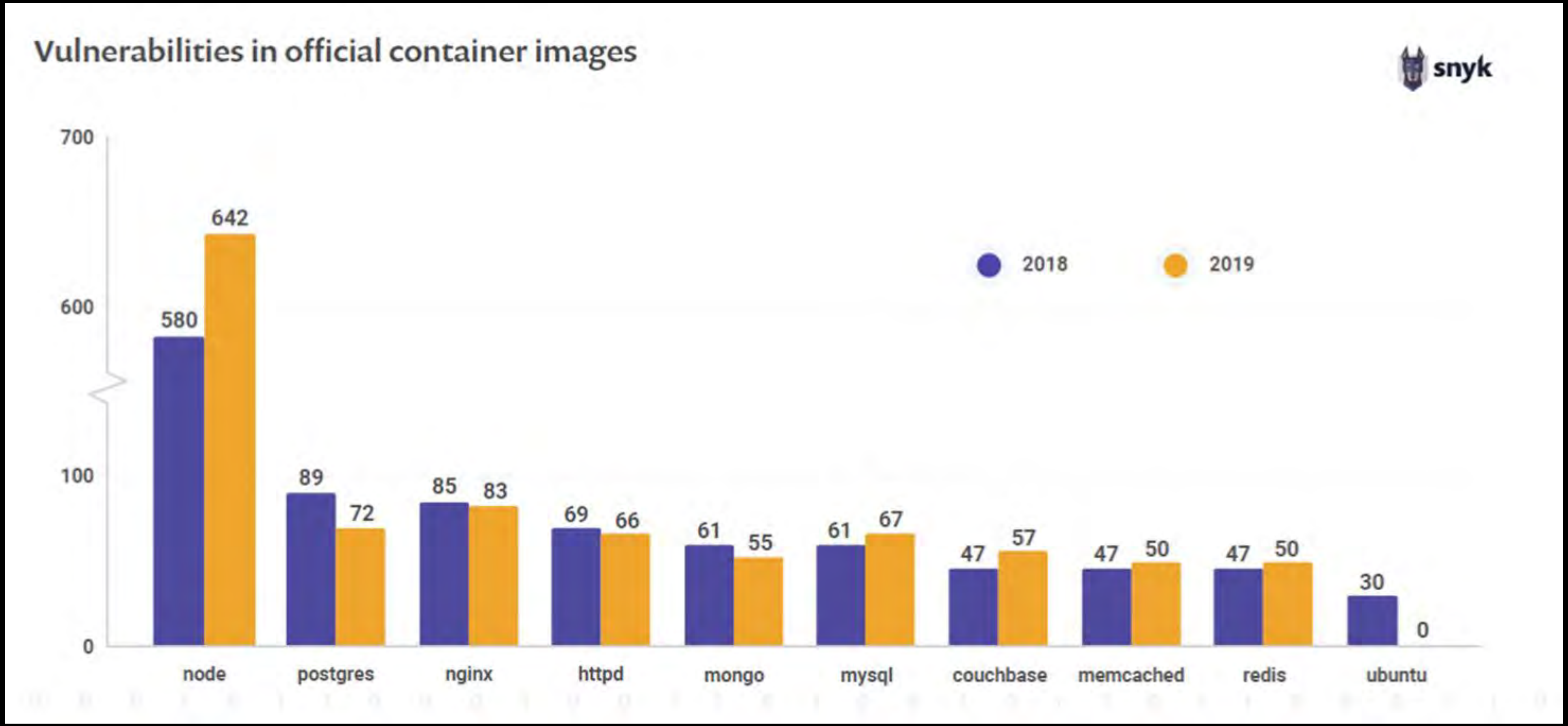
Platform	Released every	Patched every (avg.)
Chrome	1 month	14 days
Node.JS	30 months (LTS) 6 months (non-LTS)	25 days
Go	6 months Two major releases supported.	26 days
MongoDB	30 months	5 weeks
.NET	3 years (LTS) 18 months	6 weeks
Java	3 years (LTS) 6 months	12 weeks

Libraries



Source: Sonatype

Docker: hidden dependency



Source: Snyk

Is it Technical Debt?

What is debt?

- something, especially money, that is owed to someone else, or the state of owing something — *Cambridge Dictionary*
- Debt is an obligation that requires one party, the debtor, to pay money or other agreed-upon value to another party, the creditor. — *Wikipedia*
- Debt is something, usually money, borrowed by one party from another. Debt is used by many corporations and individuals to make large purchases that they could not afford under normal circumstances. A debt arrangement gives the borrowing party permission to borrow money under the condition that it is to be paid back at a later date, usually with interest. — *investopedia*

Technical Debt

«With borrowed money you can do something sooner than you might otherwise, but then until you pay back that money you'll be paying interest. I thought borrowing money was a good idea, I thought that rushing software out the door to get some experience with it was a good idea, but that of course, you would eventually go back and as you learned things about that software you would repay that loan by refactoring the program to reflect your experience as you acquired it.»

Ward Cunningham, 2009

Technical Depreciation?

Depreciation is […] the decrease in the value of assets and the method used to reallocate, or "write down" the cost of a tangible asset (such as equipment) over its useful life span. — *Wikipedia*

Unintended reduction in value of a software product over time, independent of source code changes.

or Technical Inflation?

Inflation is a general increase in the prices of goods and services in an economy […] corresponds to a reduction in the purchasing power of money. — *Wikipedia*

Unintended reduction in value of a software product over time, independent of source code changes.

or increase of Operational Costs?

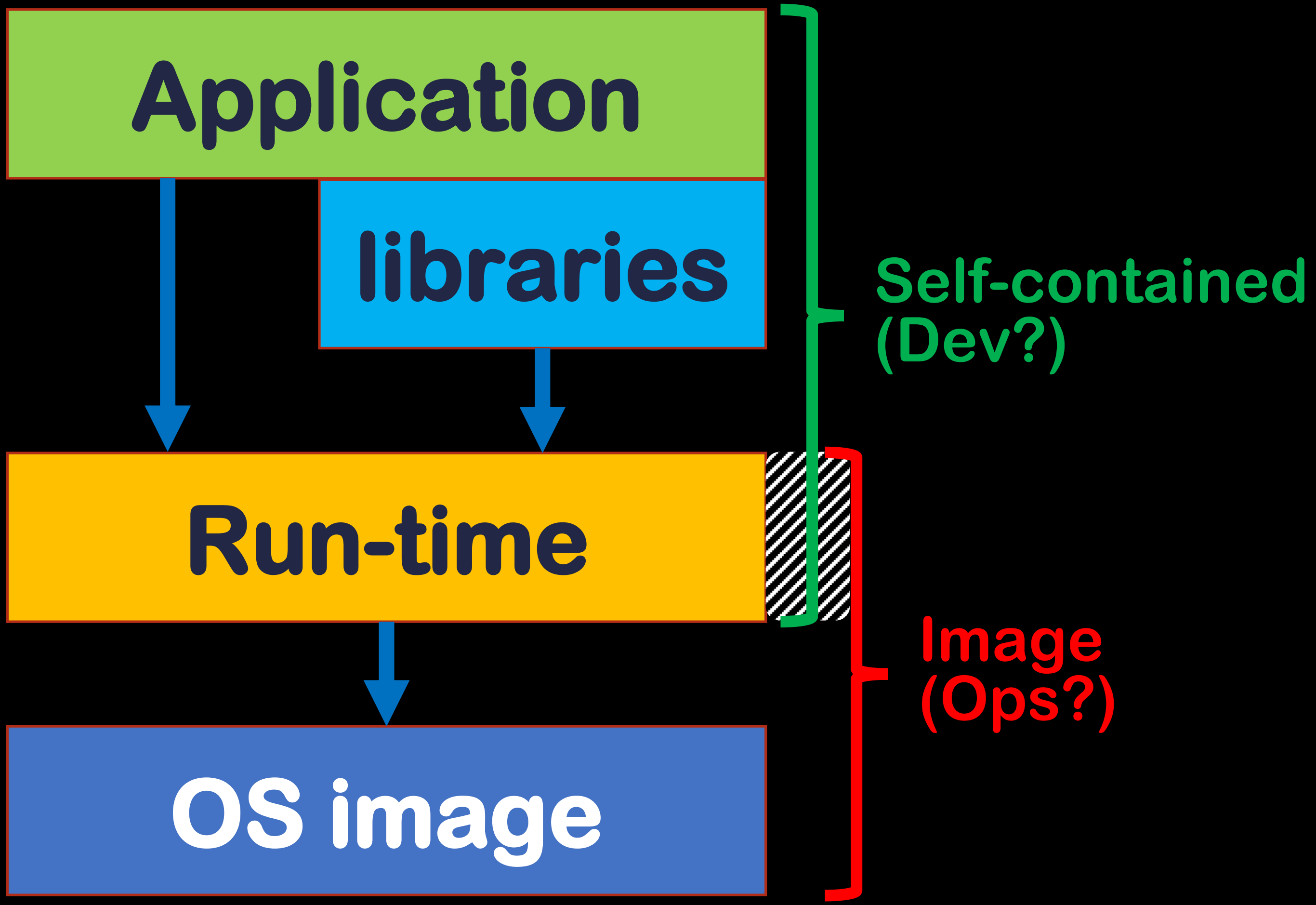
Maintenance costs to Release more often

What is Continuous Update?

Continuous Update

Necessity of frequently updating a system, independently of source code changes*.

Who manage the layers?



Application

libraries

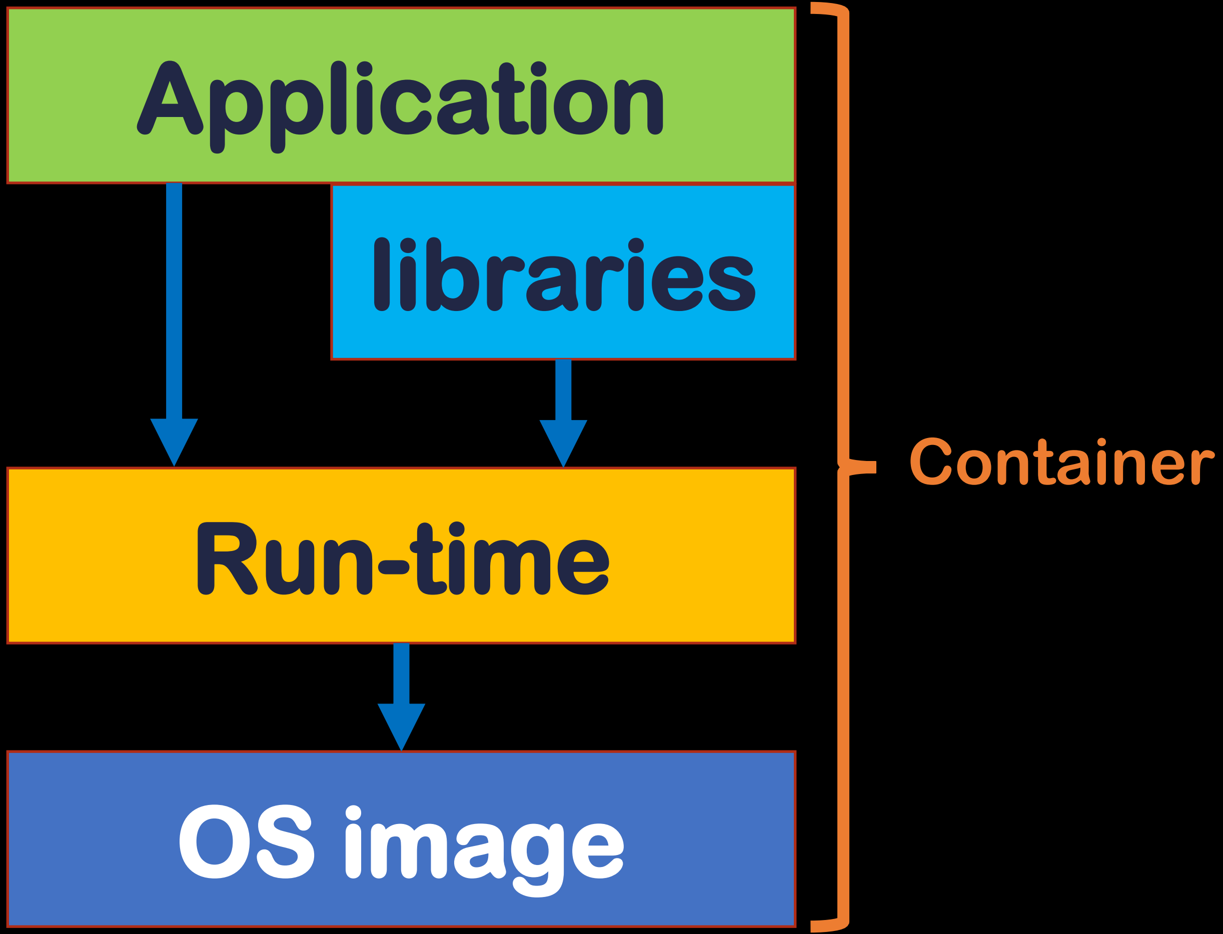
Run-time

OS image

Self-contained
(Dev?)

Image
(Ops?)

Who manage the layers?



Application

libraries

Run-time

OS image

Container

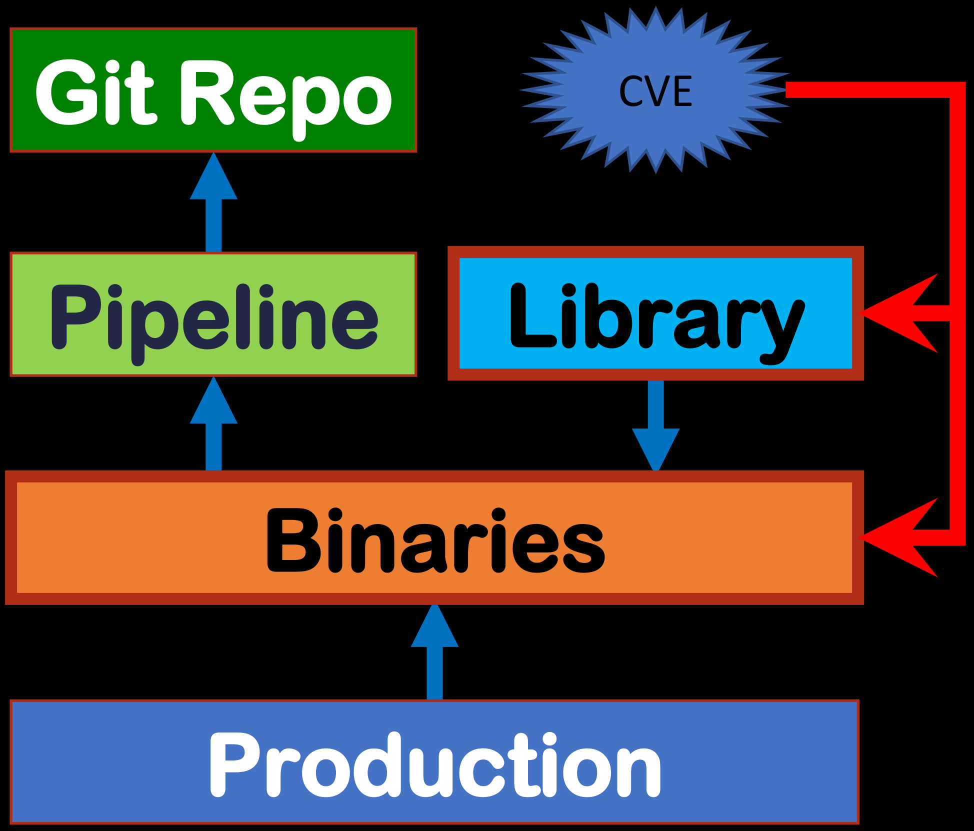
Always & everything

Image: the gerbil wheel pose by dbgg1979

Bill of Materials *on steroids*

Reverse indexes

SBOM	Library → Binaries	[SCA tool]
	O.S. API → Binaries	[SAST tool]
	Binary → Pipelines	[artifact store]
	Pipeline → Repo(s)	[pipeline tool]



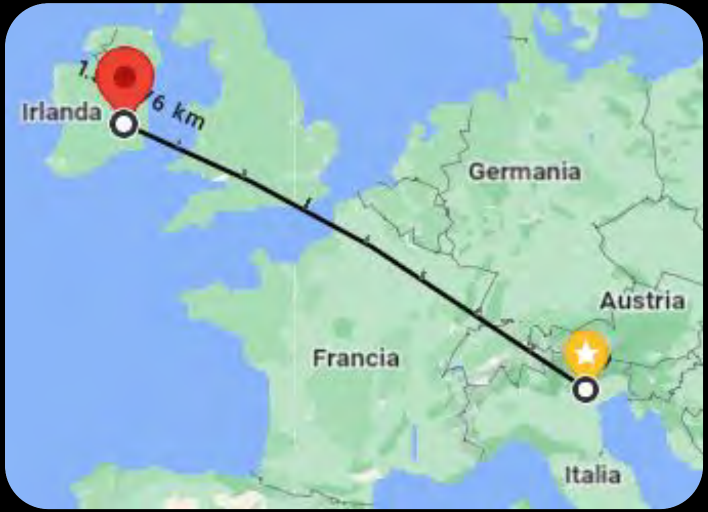
Testing, Resources, oh my!

Is Technical Debt
the right metaphor
for Continuous Update?

No, we must
rebuild Production frequently
(Continuous Update)
and it is not our fault
(aka Technical Debt)

Bio & Contacts

https://www.linkedin.com/in/giuliovian
@giulio_vian



unum sm

buildit @ wipro digital

GLASS LEWIS

AGT international

Microsoft

INFERENTIA

Artel
the e-volution people

References (1/3)

https://www.sonatype.com/resources/state-of-the-software-supply-chain-2021

https://blog.chromium.org/2021/03/speeding-up-release-cycle.html

https://nodejs.org/en/about/releases/

https://chromium.googlesource.com/chromium/src/+/refs/heads/main/docs/process/release_cycle.md

https://support.google.com/chrome/a/answer/6220366

https://dotnet.microsoft.com/en-us/platform/support/policy/dotnet-core

https://docs.fedoraproject.org/en-US/releases/lifecycle/

https://www.oracle.com/java/technologies/java-se-support-roadmap.html

https://kubernetes.io/releases/release/

https://www.mongodb.com/support-policy/software

https://heartbleed.com/

Why Every Business Is a Software Business — Watts S. Humphrey Informit, Feb 22, 2002
http://www.informit.com/articles/article.aspx?p=25491

https://en.wikipedia.org/wiki/Watts_Humphrey

https://www.sonatype.com/resources/state-of-the-software-supply-chain-2021

https://www.shopify.com/enterprise/global-ecommerce-statistics

References (2/3)

https://blog.cloudflare.com/popular-domains-year-in-review-2021/
https://radar.cloudflare.com/year-in-review-2021
https://snyk.io/blog/net-open-source-security-insights/
https://www.contrastsecurity.com/the-state-of-the-oss-report-2021
https://octoverse.github.com/static/github-octoverse-2020-security-report.pdf
https://www.soa.org/globalassets/assets/files/resources/research-report/2020/quantification-cyber-risk.pdf
https://www.soa.org/globalassets/assets/files/resources/research-report/2020/exposure-measures-cyber-insurance.pdf
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
https://www.verizon.com/business/resources/reports/dbir/
https://www.accenture.com/us-en/insights/security/cost-cybercrime-study
https://www.ibm.com/security/data-breach
https://go.snyk.io/SoOSS-Report-2020.html
https://www.amazon.co.uk/Accelerate-Software-Performing-Technology-Organizations/dp/1942788339
https://www.sciencedirect.com/science/article/abs/pii/0164121279900220
https://daverupert.com/2020/11/technical-debt-as-a-lack-of-understanding/

References (3/3)

https://wiki.owasp.org/images/b/bd/Software_Composition_Analysis_OWASP_Stammtisch_-_Stanislav_Sivak.pdf

https://googleprojectzero.blogspot.com/

https://googleprojectzero.blogspot.com/2022/04/the-more-you-know-more-you-know-you.html

https://github.com/nodejs/node/blob/master/doc/changelogs/CHANGELOG_V14.md

https://dotnet.microsoft.com/en-us/download/dotnet/3.1

https://docs.mongodb.com/upcoming/release-notes/5.0/

https://www.devsecops.org/

https://github.com/golang/go/wiki/Go-Release-Cycle

https://go.dev/doc/devel/release

https://libraries.io/data

https://github.com/devopsenterprise/2021-virtual-us/blob/main/Bryan%20Finster%20-%20DOES%202021%20-%20Misuse%20and%20Abuse%20DORA%20Metrics.pdf

https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

http://wiki.c2.com/?WardExplainsDebtMetaphor

Thank you!