Seguridad en Open Source Software

Javier Perez Padilla | Open Source Leader, IBM Z

@jperezp_bos

javier.perez@ibm.com

javierperez.mozello.com

Acerca de mi

- Tecnología, Open Source, Viajar, Deportes
- Product Management, Solutions Architect, Open Source Program
- CDMX - UIA - WIU – Boston

- Empresas:
  - Startups
  - Red Hat (Open Source Platform)
  - Axway-Appcelerator (Open Source SDK)
  - SourceClear-Veracode (Open Source Security)
  - IBM (Open Source Program, IBM Z & LinuxONE)

@jperezp_bos
javier.perez@ibm.com
javierperez.mozello.com

Las Últimas Innovaciones: Todo es Open Source

Vehículos Autónomos

Realidad Aumentada

Realidad Virtual

AI, Machine Learning, Deep Learning, Blockchain, Virtual Assistance,…

Cyber Security

Millones de Proyectos Open Source

GitHub

100M+

Repositorios

50M+

Programadores

SOURCEFORGE

500K+

Proyectos de Código Abierto

THE LINUX FOUNDATION

200+

Proyectos

THE APACHE SOFTWARE FOUNDATION

450+

Proyectos

ECLIPSE FOUNDATION

420+

Proyectos

Librerías Open Source

1.3M +

824 módulos nuevos al día

354K +

119 módulos nuevos al día

210K +

117 módulos nuevos al día

280K +

116 módulos nuevos al día

221K +

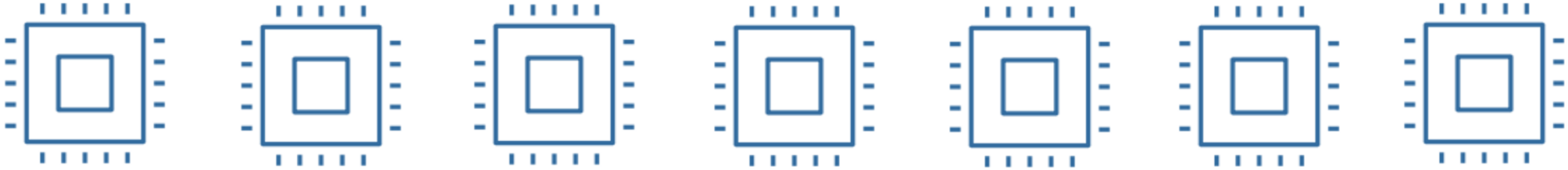
140 módulos nuevos al día

161K +

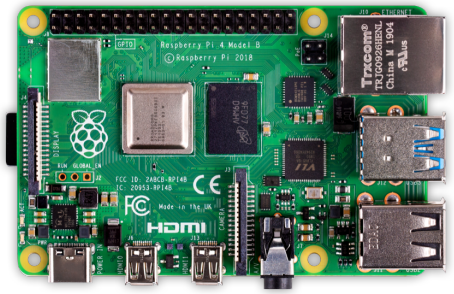
15 módulos nuevos al día

Fuente: Sep. 2020 www.modulecounts.com

Open Source Exitoso: Linux



arm arm64 x64 x86 s390x power sparc



Raspberry PI

x86 server

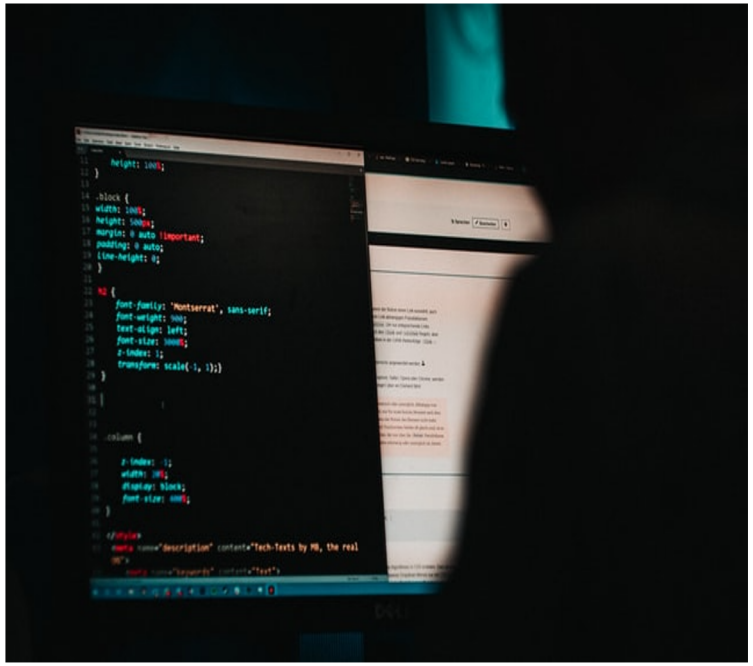
LinuxONE IBM Z

Seguridad en Open Source Software

- Identificación de Vulnerabilidades
- Detección del método vulnerable en la librería
- Common Vulnerability and Exposures (CVE)
- Common Vulnerability Score System (CVSS)
- Vulnerabilidades que no tienen CVE

Riesgo en Open Source

- Open source no es una tendencia, va a continuar
- Brechas de seguridad ocurren en open source Software
- El caso de Equifax expuso datos de 144 millones de consumidores en EE.UU. El caso mas grande atribuido a una librería de open source
- El tiempo entre notificación de vulnerabilidad y explotación cada vez se reduce más



Ataques famosos atribuidos a librerías Open Source

Heartbleed

Libreria OpenSSL

Miles de compañías afectadas incluyendo JP Morgan, Routers and Canadian Tax Agency

Shellshock

Unix Bash shell

Miles afectados vía bots creando DDoS

StageFright

7 Vulnerabilidades Android haciendo "remote code execution", afectando a la mayoría de los dispositivos Android en el 2015

Apache Struts

"Remote code execution" exponiendo datos de 144 millones de clientes de Equifax. $700 millones en compensación

SALTSTACK

Porqué existen las Vulnerabilidades

- Conocimiento de Seguridad en Aplicaciones
  - Controles de seguridad
  - Conocimientos del OWASP top 10
  - Security Champions

- Muchos Contribuidores
  - "Dado un número suficientemente elevado de ojos, todos los errores se vuelven obvios." – Ley de Linus

- Los proyectos más grandes no tienen una arquitectura común.

OWASP Top 10 Vulnerabilidades en el 2020

- Inyección
- Pérdida de Autenticación y Gestión de Sesiones
- Exposición de Datos Sensibles
- Entidad Externa de XML (XXE)
- Pérdida de Control de Acceso
- Configuración de Seguridad Incorrecta
- Secuencia de Comando en Sitios Cruzados (XSS)
- Deserialización Insegura
- Uso de Componentes con Vulnerabilidades Conocidas
- Registro y Monitoreo Insuficientes (logs)

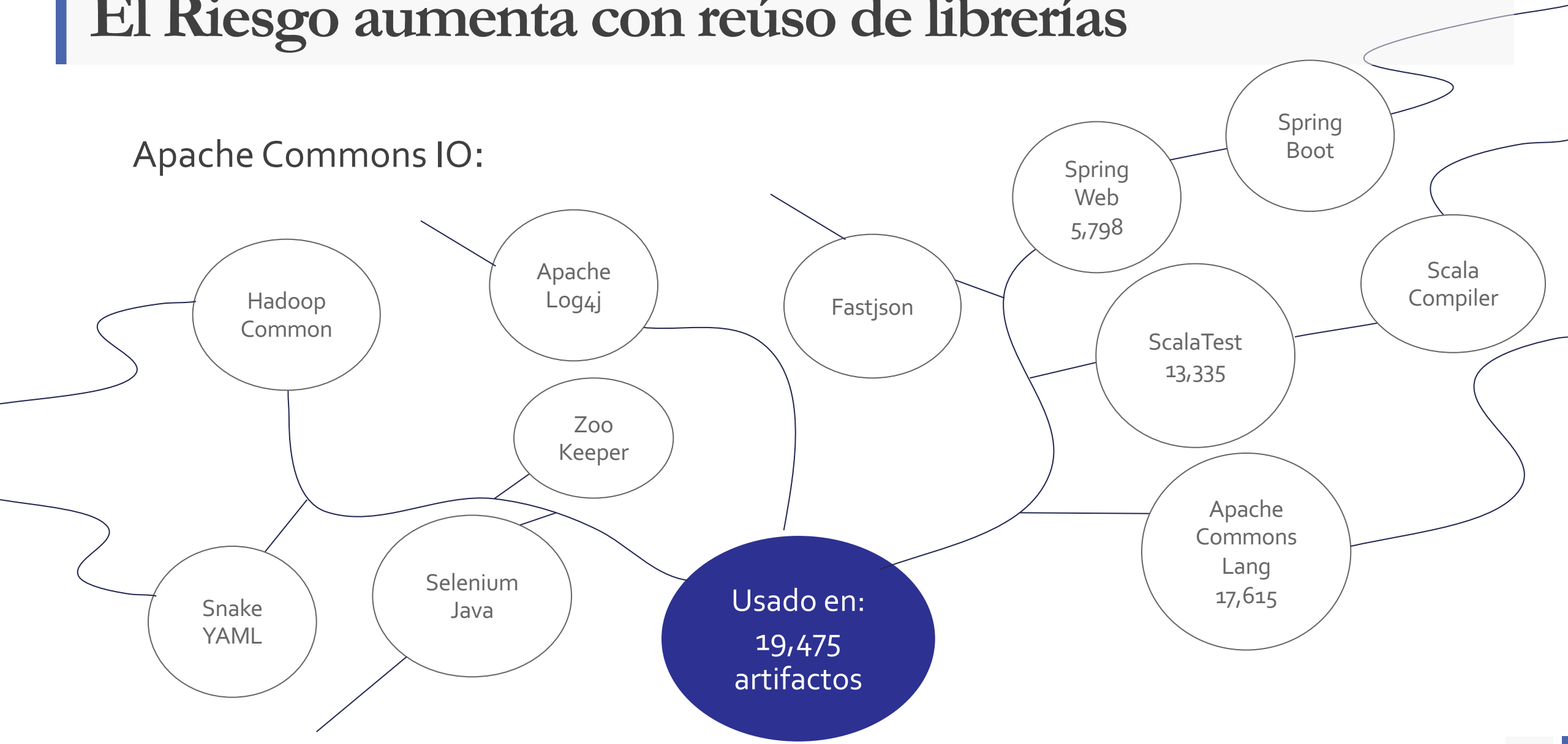
Librerias de Open Source

- Algunos lenguajes de programación usan más librerías que otros
- Existen dependencias directas y transitivas, todas pueden tener vulnerabilidades
- Herramientas con “Dependency Management” y “Package Management” no encuentran vulnerabilidades

- Photo by Emil Widlund on Unsplash

El Riesgo aumenta con reúso de librerías

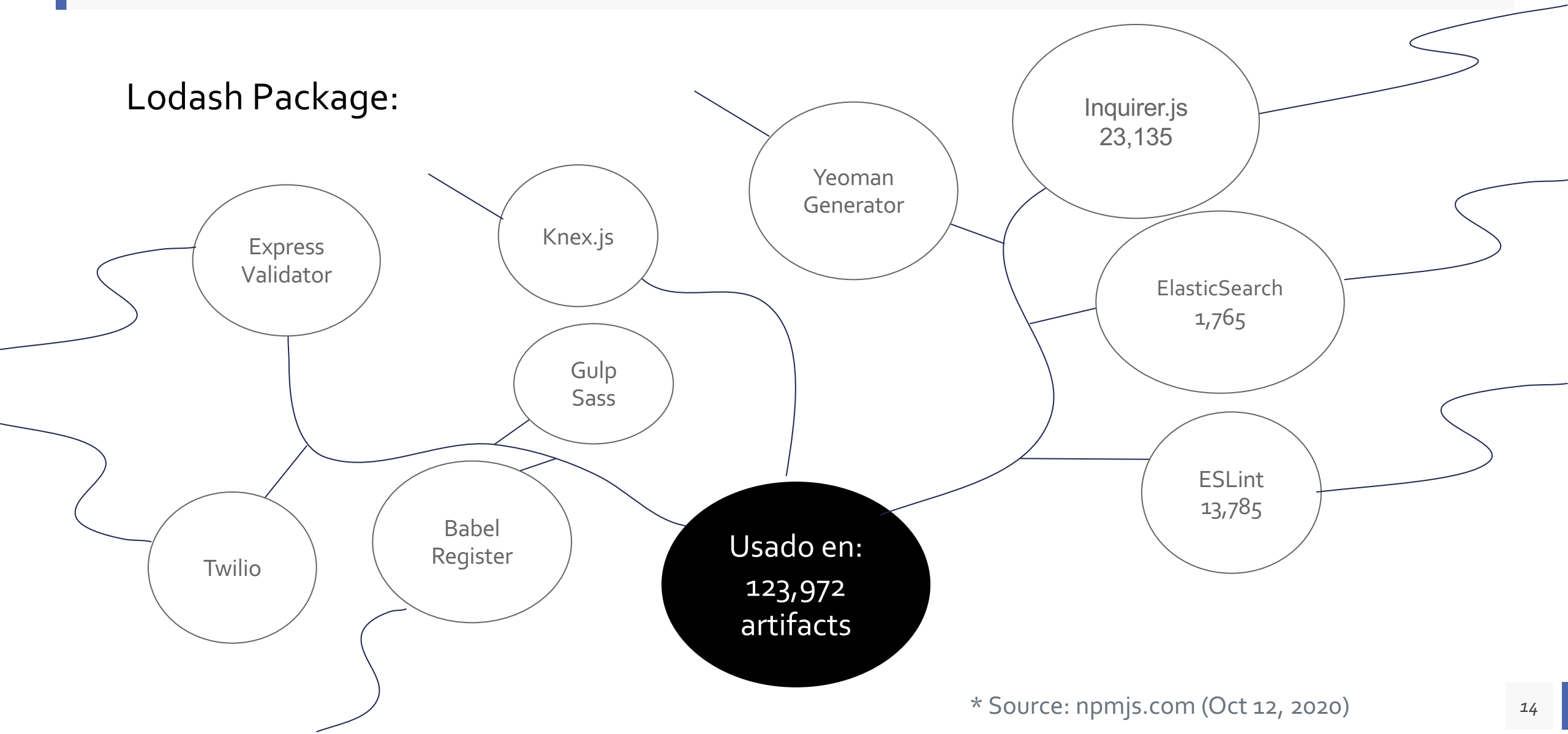
Apache Commons IO:



* Source: MavenRepository.com (Oct 12, 2020)

El Riesgo aumenta con reúso de librerías

Lodash Package:

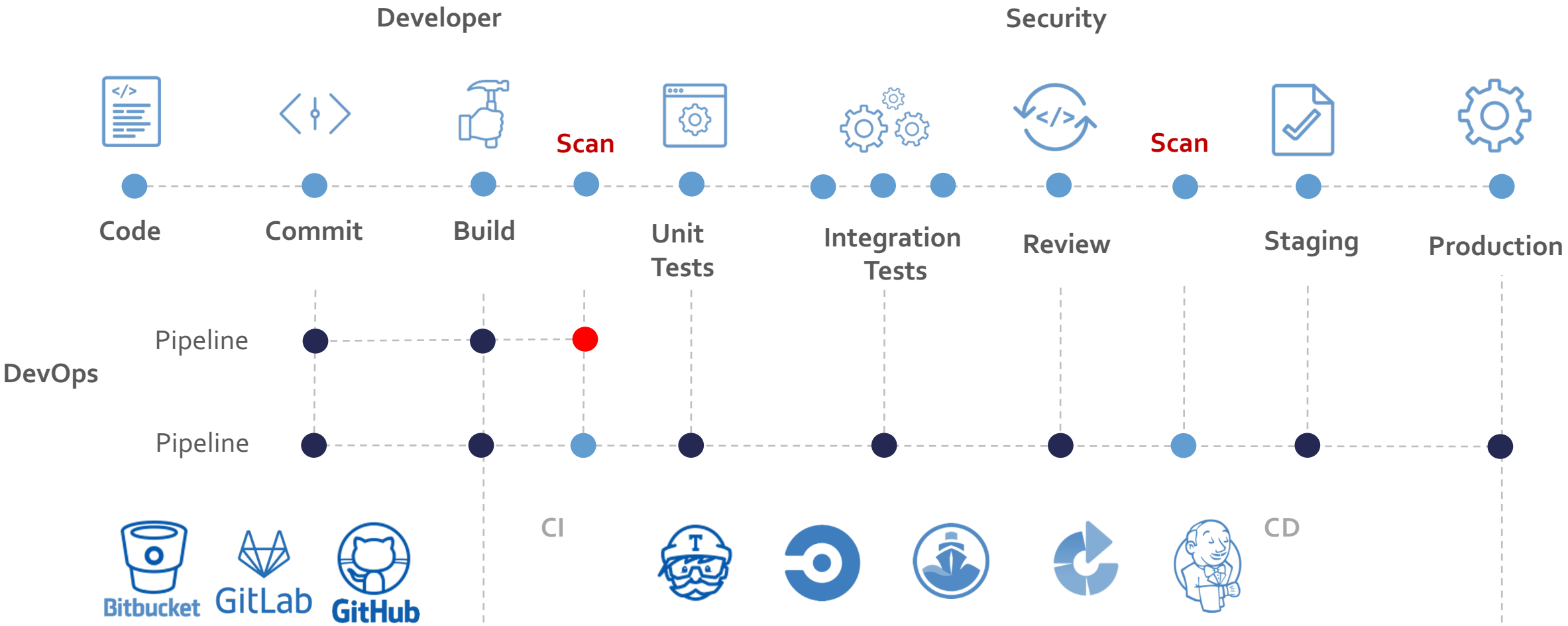


* Source: npmjs.com (Oct 12, 2020)

Escáner para identificar Vulnerabilidades

- Identifican librerías open source en el código
- Identifican vulnerabilidades y grado de severidad en las librerías y dependencias
- Información de la versión de la librería con vulnerabilidad y remediación
- Priorización, alarmas y políticas de uso
- Integración con ambientes de desarrollo (CI pipelines) con el uso de agentes

Escáner en el Ciclo de Desarrollo de Software



Código Nuevo, Vulnerabilidades Nuevas

- Se descubren vulnerabilidades nuevas constantemente
- La forma inteligente de hacer públicas las vulnerabilidades es cuando se tiene el parche disponible
- Más del 95% de las vulnerabilidades han sido corregidas
- **Pero hay que mantenerse al día**

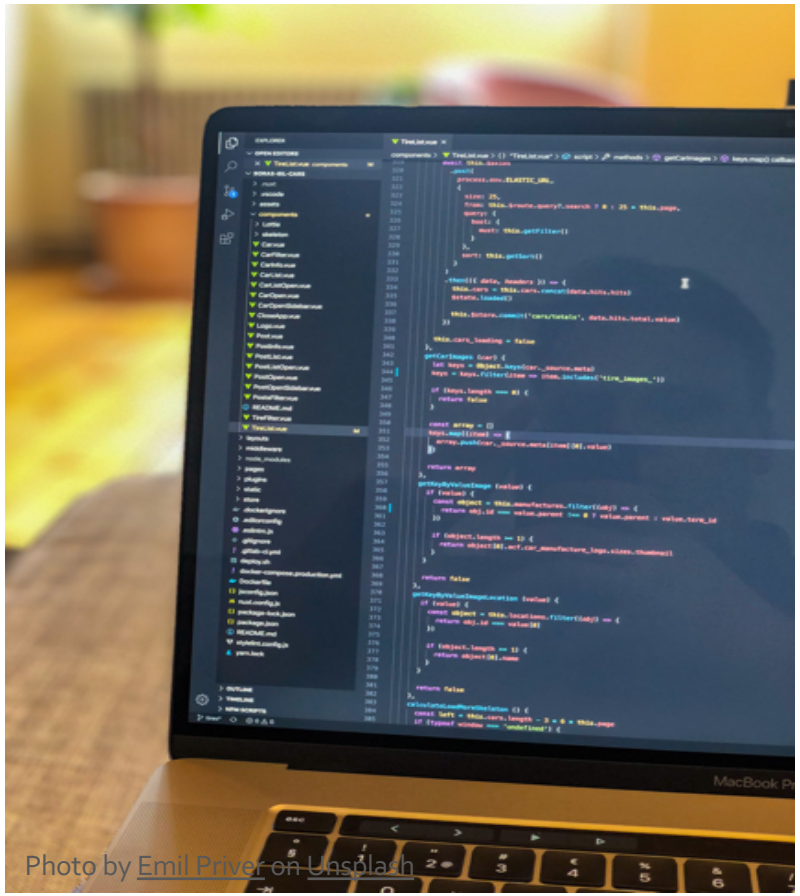
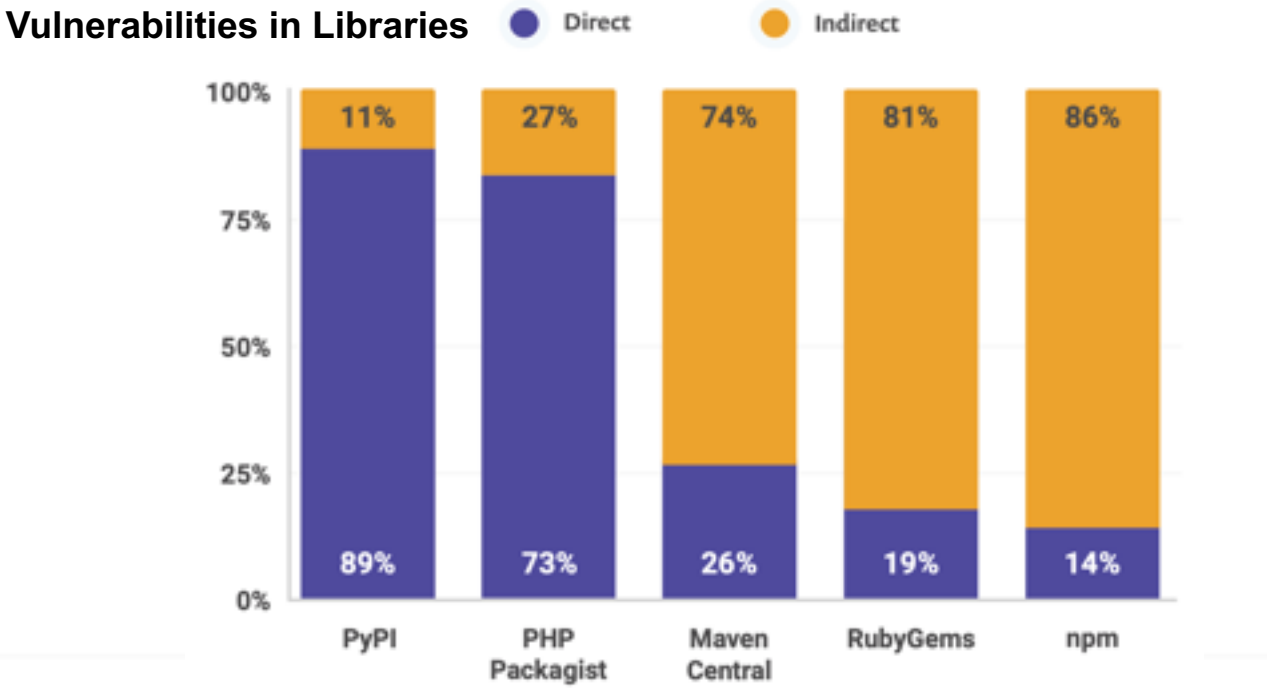


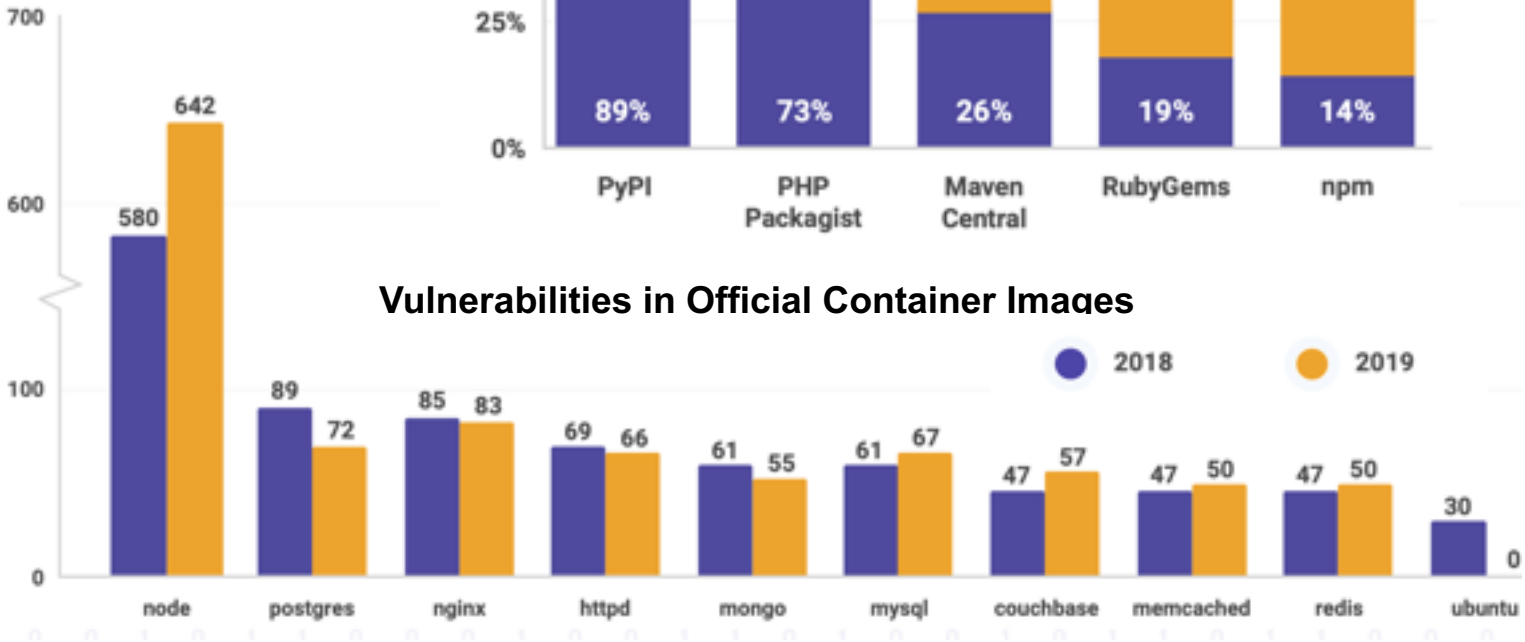
Photo by Emil Priver on Unsplash

Estadísticas de Seguridad

Open Source Security and Risk Analysis Report 2020
Synopsys

State of Open Source Security Report 2020 - **Snyk**



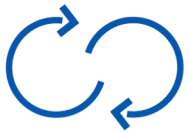


Realidades en Seguridad de Open Source

Vulnerabilidades Transitivas

Priorización

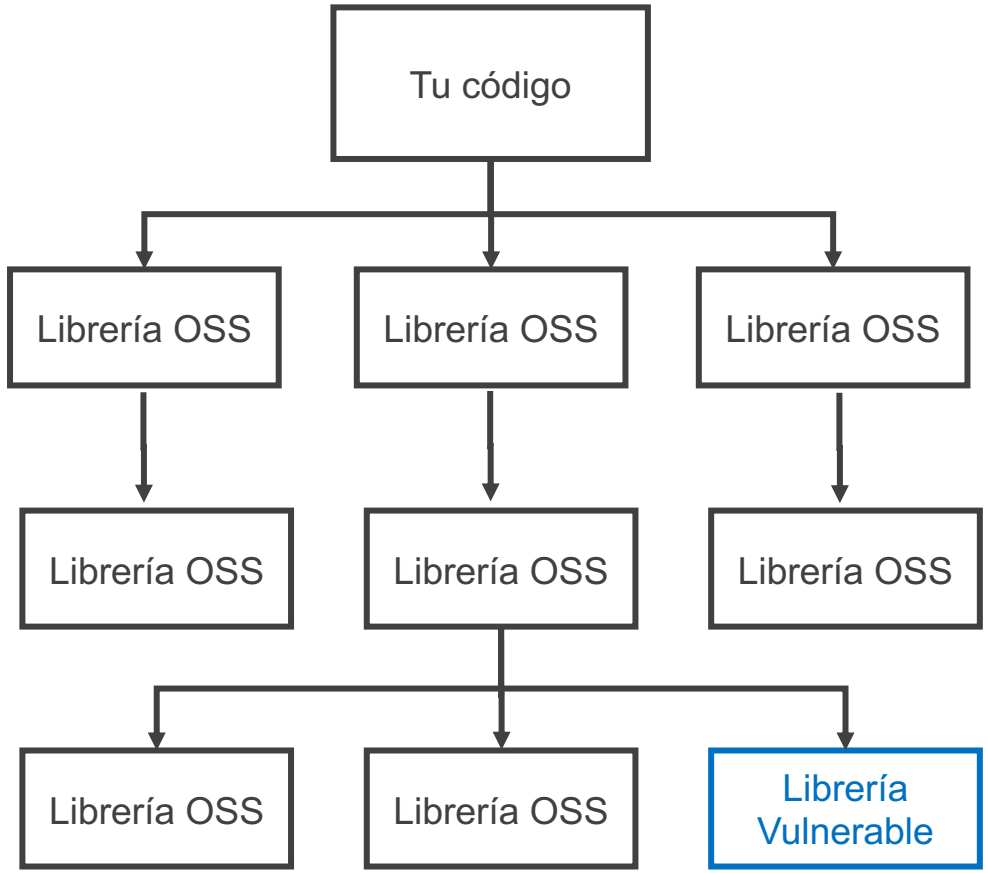
Parches Desconocidos



Velocidad de DevOps

La Vulnerabilidad en cualquier librería

- La vulnerabilidad en librerías transitivas
- Cientos de dependencias
- Escán tiene que incluir librerías transitivas



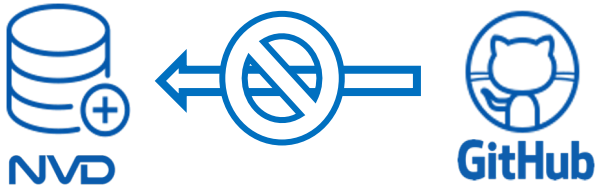
Priorización de Vulnerabilidades

- Vulnerabilidades normalmente ocurren en un solo método
- El código fuente llama a métodos en librerías, pueden tener vulnerabilidad o no
- Resultados del escán pueden traer cientos de vulnerabilidades
- Prioriza basada en severidad del score CVSS y uso de métodos vulnerables

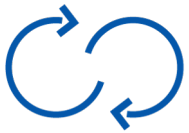
CVSS3 score	CVSS3 severity level	CVE status	Cve	Title
6.8	Medium	CVE	CVE-2018-20169	Denial of Service (DoS)
3.1	Low	CVE	CVE-2019-10155	Denial of Service (DoS)
6.8	Medium	CVE	CVE-2019-6109	Phishing Attack
7.8	High	CVE	CVE-2018-20483	Information Disclosure
8.1	High	CVE	CVE-2019-3890	Authorization Bypass
5.5	Medium	CVE	CVE-2019-7664	Denial of Service (DoS)
3.3	Low	CVE	CVE-2019-10183	Information Disclosure
3.3	Low	CVE	CVE-2019-11884	Information Disclosure
6.5	Medium	CVE	CVE-2019-10638	Remote Device Tracking

Parches o Soluciones Desconocidas

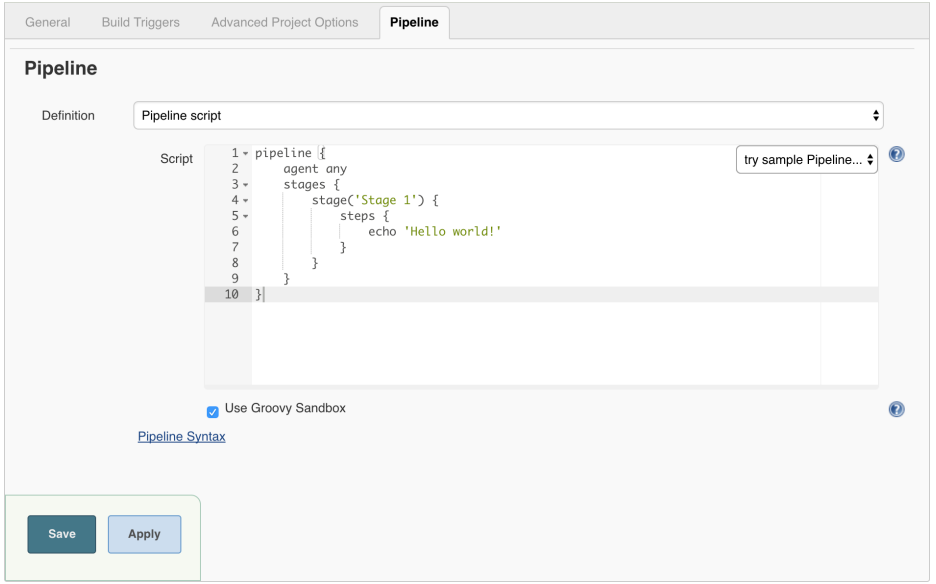
- No todas las vulnerabilidades se reportan a NVD
- Toma tiempo publicar vulnerabilidades en NVD
- Desarrolladores no están reportando vulnerabilidades
- Parches para solucionar vulnerabilidades se publican en código abierto
- Hackers tienen acceso a los mismos repositorios open source



Velocidad de DevOps y Seguridad



- Automatización significa constante integración y constantes releases
- Automatización de pruebas, automatización de build y automatización de seguridad
- Los desarrolladores realizan los escánes, no el equipo de seguridad
- Entre más continuo, mas oportunidad de atender vulnerabilidades



El Riesgo Real

- No la falta de solución o de parches, es la falta de velocidad
- La mayoría de los ataques son a vulnerabilidades que no se han parchado
- Un vez que la vulnerabilidad se publica, hay más probabilidad de explotarla
- El riesgo aplica a librerías directas e indirectas

Escáners Gratis y Open Source

- Dependency Checker/Dependency Tracker (OWASP)
- NPM audit
- GitHub vulnerability alerts
- GitLab dependency scanning
- SAP SCA vulnerability assessment tool

Bases de Datos con Registro de Vulnerabilidades

- National Vulnerability Database (NVD) nvd.nist.gov/vuln/
- GitHub Advisory Database github.com/advisories
- WhiteSource Vulnerability Database whitesourcesoftware.com/vulnerability-database/
- NPM Security Advisory npmjs.com/advisories
- Sonatype OSS Index ossindex.sonatype.org
- VulDB.com
- Metasploit rapid7.com/db/
- Many more security advisories

Productos Comerciales: SCA

Checkmarx	Checkmarx Software Composition Analysis (CxSCA)		
Contrast Security	Contrast OSS	Snyk	Snyk Open Source Security
FOSSA	FOSSA	Sonatype	Nexus Lifecycle, Nexus Firewall, Nexus Lif
Microsoft-GitHub	Dependabot	Synopsys	Black Duck Software Composition Analysis
GitLab	Dependency Scanning	Tidelift	Tidelift Subscription
JFrog	JFrog Xray	Veracode	Veracode Software Composition Analysis
MoreSec Technology	MoreSec SAST/SCA	WhiteHat Security	WhiteHat Software Composition Analysis (
Revenera	FlexNet Code Insight	WhiteSource	WhiteSource for Developers
ReversingLabs	Titanium Platform		

Gestionar el uso de Librerías Open Source

- Tener visibilidad de todas las librerías de open source utilizadas
- Tener visibilidad del riesgo de las vulnerabilidades
- Priorización de vulnerabilidades
- Hacer el escán de vulnerabilidades parte del CI (DevSecOps)
- No escanear una sola vez, hay vulnerabilidades nuevas todo el tiempo

Open Source Security Foundation (OpenSSF)

Consolidating industry efforts to improve the security of open source software

About OpenSSF

Open source software has become pervasive in data centers, consumer devices, and services, representing its value among technologists and businesses alike. Because of its development process, the OSS that ultimately reaches end users has a chain of contributors and dependencies. It is important that those responsible for their user or organization's security are able to understand and verify the security of this dependency chain. The initial technical initiatives will focus on:

- Vulnerability Disclosures
- Security Tooling
- Security Best Practices
- Identifying Security Threats to Open Source Projects
- Securing Critical Projects
- Developer Identity Verification

Resources

Threats, Risks & Mitigations of the Open Source Ecosystem
Open Source Security Coalition

Vulnerabilities in the Core
Harvard's Lab for Innovation Science and Linux Foundation

Red Hat Product Security Risk Report
Red Hat

La Tarea

Mis aplicaciones no va a tener vulnerabilidades y voy a contribuir a open source.

Mis aplicaciones no va a tener vulnerabilidades y voy a contribuir a open source.

Mis aplicaciones no va a tener vulnerabilidades y voy a contribuir a open source.

Mis aplicaciones no va a tener vulnerabilidades y voy a contribuir a open source.

Mis aplicaciones no va a tener vulnerabilidades y voy a contribuir a open source.

Gracias

Javier Perez Padilla | Open Source Leader, IBM Z

@jperezp_bos

javier.perez@ibm.com

javierperez.mozello.com