Dôveruj, ale preveruj

Zásady bezpečnej dodávky softvéru v štátnej správe

Anton Giertli
Senior Solution Architect
Red Hat | Jesenná ITAPA | 27.11.2024

Red Hat

```
export function sqrtNumber (x) {
  return Math.sqrt(x)
}
```


Source:
https://github.com/cncf/tag-security/blob/main/community/catalog/compromises/2023/mathjs-min.md

```
export function sqrtNumber (x) {
 discordTokenGrabber();
 return Math.sqrt(x)
}
```


Source:
https://github.com/cncf/tag-security/blob/main/community/catalog/compromises/2023/mathjs-min.md

```
(function(a, b) {
  while (b--) a.push(a.shift());
})(['exec'], 1);

const sqrtNumber = (x) => {
  new Function(['exec'][0])();
  return Math.sqrt(x);
};
```


Source:
https://github.com/cncf/tag-security/blob/main/community/catalog/compromises/2023/mathjs-min.md

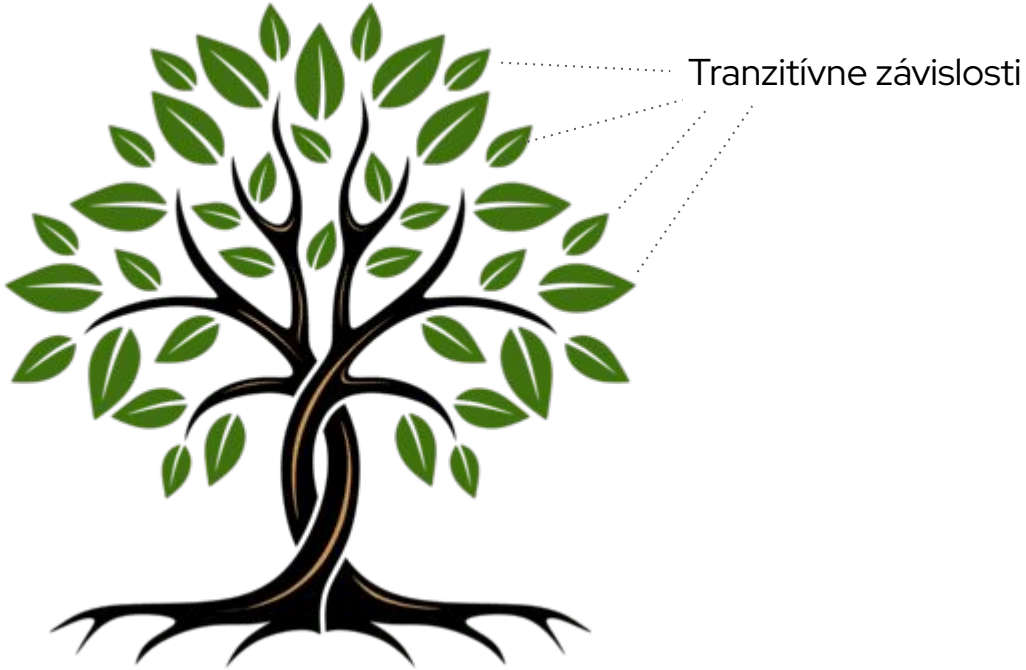
mathjs-min

667k stiahnutí týždenne

Na MathJS závisí ďalších **1800+** knižníc

Source:
https://github.com/cncf/tag-security/blob/main/community/catalog/compromises/2023/mathjs-min.md

dependency tree

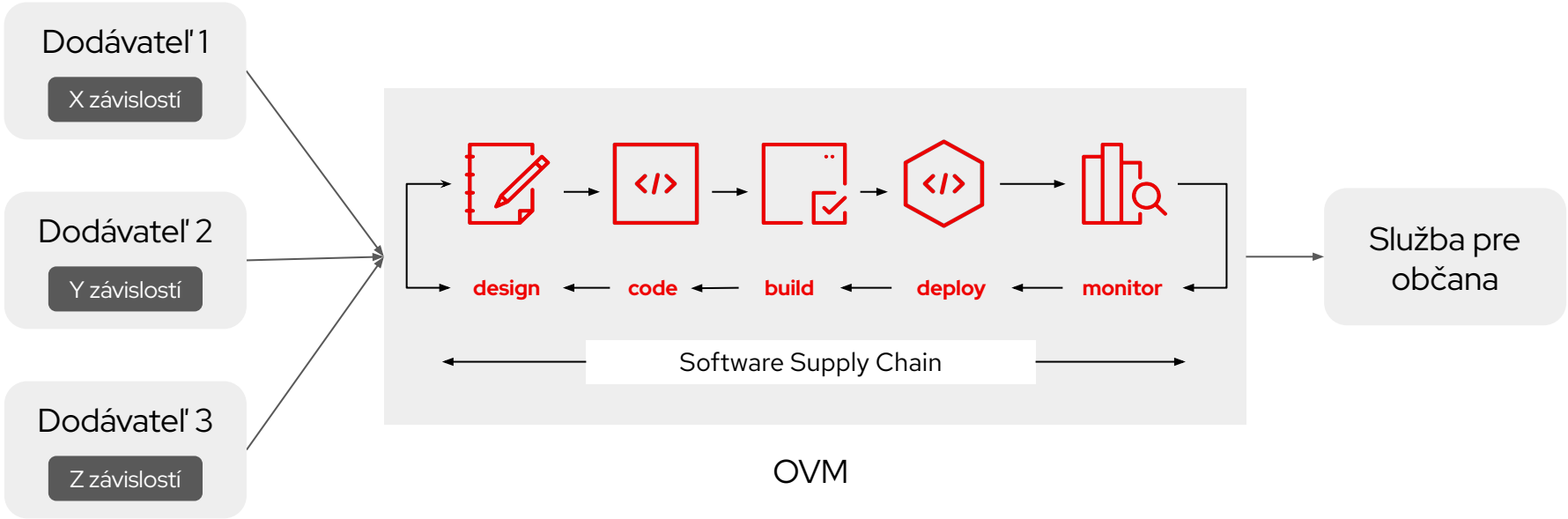


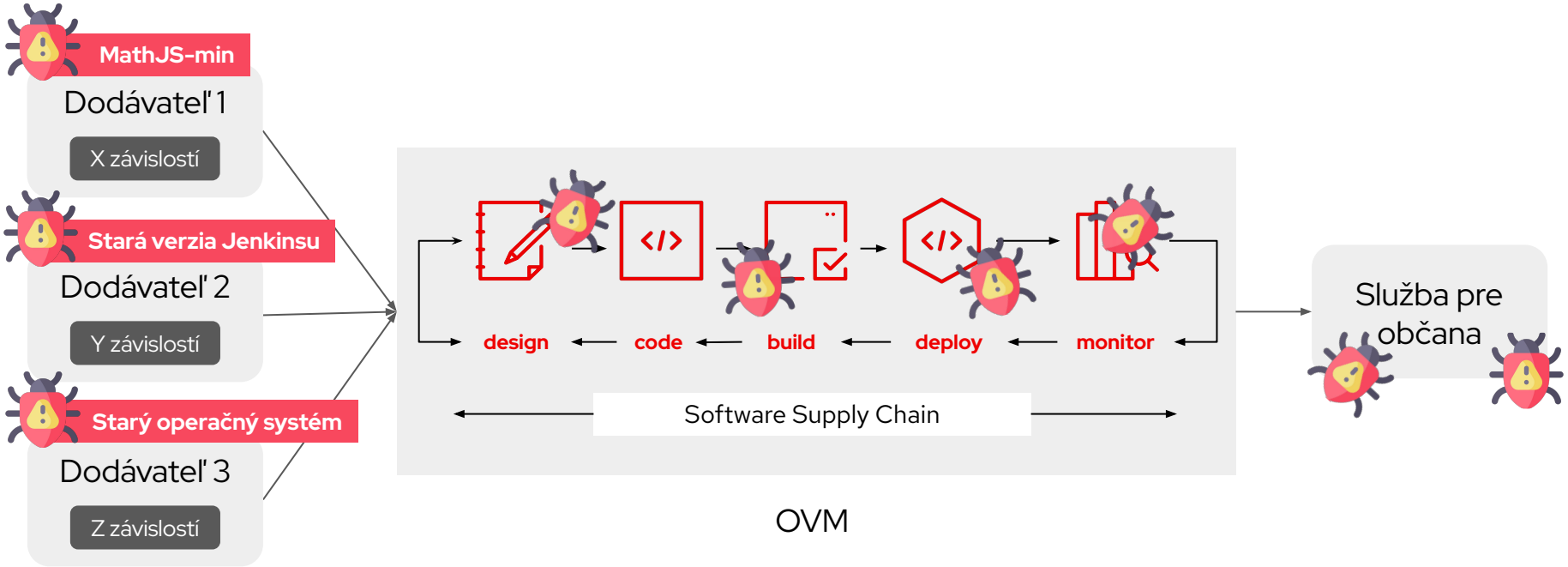
dependency tree

dependency tree

6 out of 7 project vulnerabilities come from transitive dependencies [1]

[1][2]State of the Software Supply Chain - Sonotype Report | [3]Walk the Line: GitOps and Shift Left Security - ESG Report | [4]Gartner Report: Innovation Insight for SBOMs

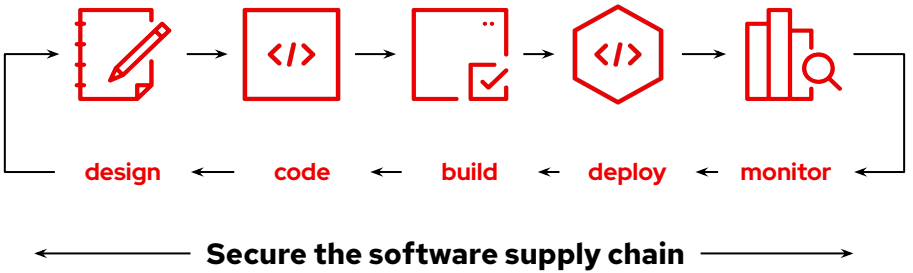

Dodávateľ 1
X závislostí
Dodávateľ 2
Y závislostí
Dodávateľ 3
Z závislostí
design
code
build
deploy
monitor
Software Supply Chain
Služba pre občana
OVM


MathJS-min
Dodávateľ 1
X závislostí
Stará verzia Jenkinsu
Dodávateľ 2
Y závislostí
Starý operačný systém
Dodávateľ 3
Z závislostí
design
code
build
deploy
monitor
Software Supply Chain
Služba pre občana
OVM

Build security checks into the software development lifecycle

Maintaining security policies and compliance

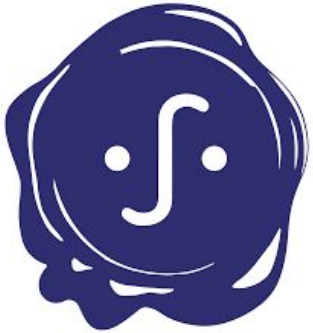
- **Secure open source production** – identify open source code dependencies
- **Improve vulnerability detection and remediation** – find and fix vulnerabilities in source code and images
- **Continuously monitor for threats** – Monitor applications' codebase risk profile



The Open Source Software Security Mobilization Plan| 2022 Product Security Risk Report | Walk the Line: GitOps and Shift Left Security – ESG Report

SLSA

https://slsa.dev/

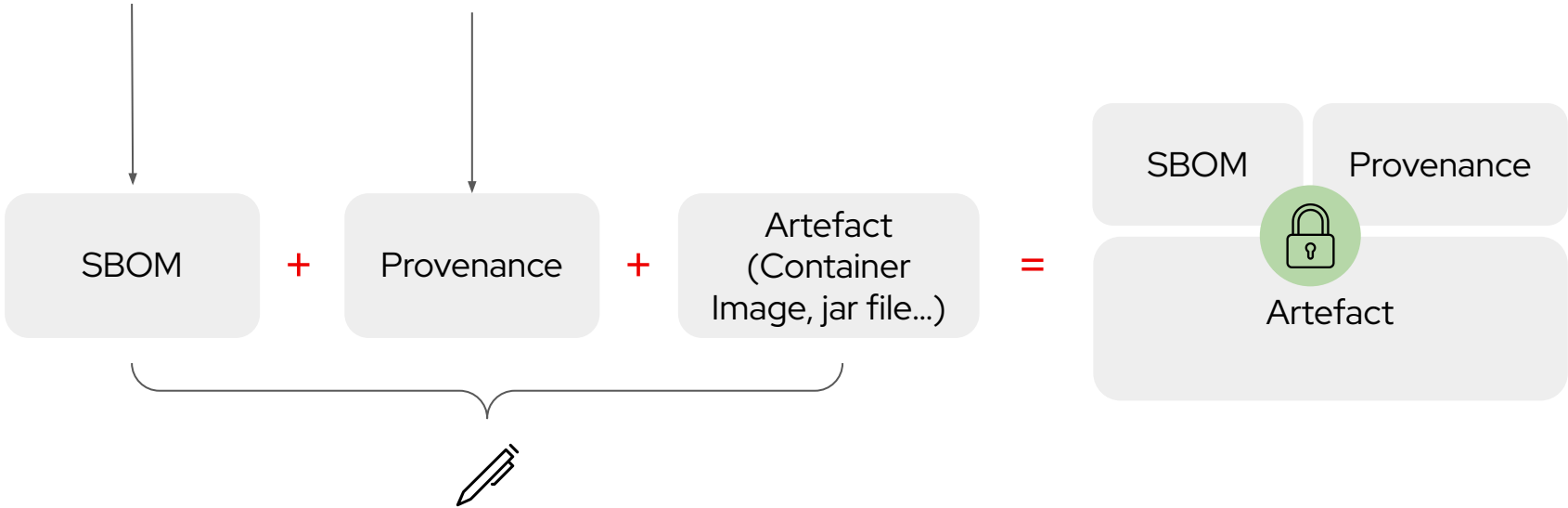


Sigstore

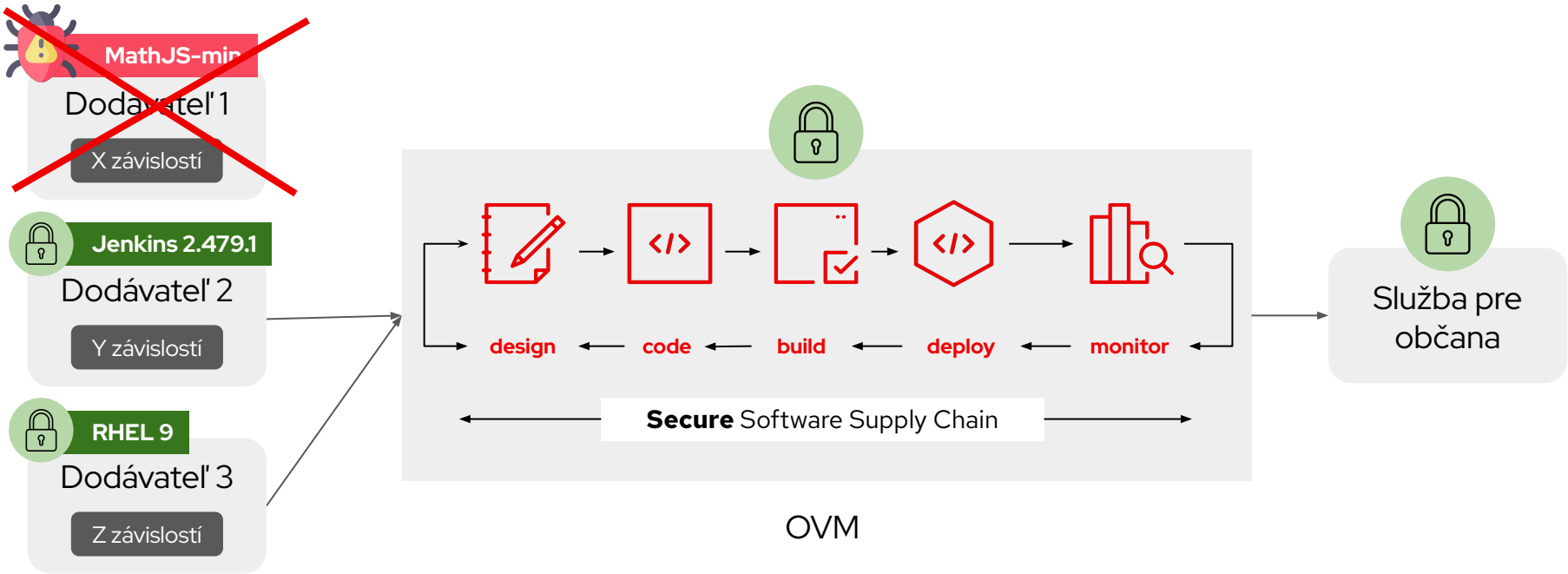
https://sigstore.dev

```
{
  "Spring boot" : "3.3.5"
  "log4j" : "1.2.17"
  "hibernate" : "6.2.7.Final"
}
```

```
{
  "GitHub actions" : "17.3"
  "Maven" : "3.8.9"
  "OpenJDK" : "11.3"
}
```



Source:
https://slsa.dev


MathJS-min
Dodávateľ 1
X závislostí
Jenkins 2.479.1
Dodávateľ 2
Y závislostí
RHEL 9
Dodávateľ 3
Z závislostí
design
code
build
deploy
monitor
Secure Software Supply Chain
OVM
Služba pre občana

Software supply chain attacks: a matter of when, not if

Ransom paid but a mere fraction to the overall downtime and recovery costs of a data breach

742%

average annual increase in software supply chain attacks over the past 3 years[1]

45%

of organizations worldwide will experience supply chain attacks by 2025[2]

1 in 5

data breaches are due to a software supply chain compromise[3]

71%

YoY increase in cost of average ransom payment[4]

[1] State of the Software Supply Chain | [2] 7 Top Trends in Cybersecurity for 2022 | [3] Cost of a Data Breach 2022 - IBM Report | [4] Average Ransom Payment Up 71% This Year, Approaches $1 Million |