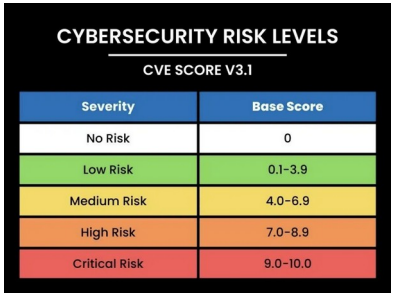
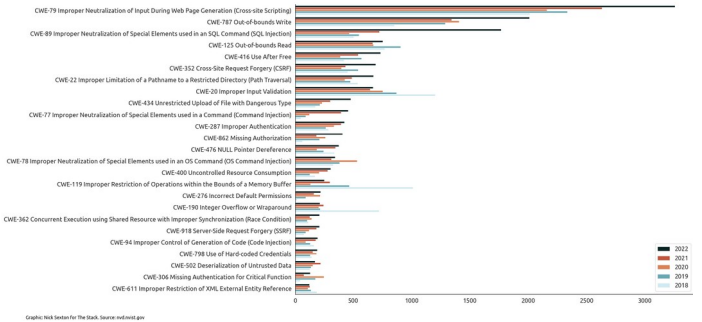
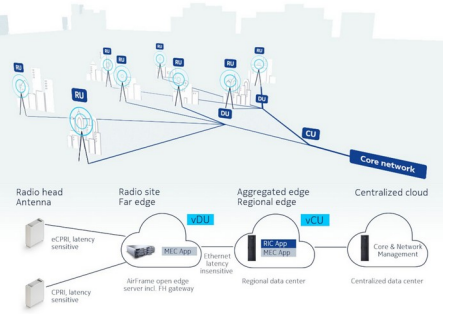






Software security vulnerabilities in practice

Jan Žižka, M.Sc.
Principal Technical Leader at Nokia
DMTS, Nokia Bell Labs
PhD student at FI MUNI

MITRE

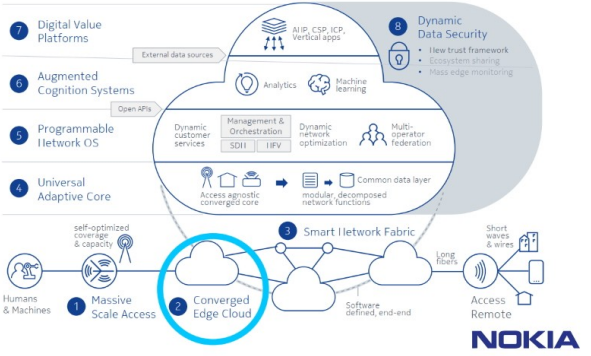
trivy

NATIONAL VULNERABILITY DATABASE
NVD

CVE®

Jan Žižka

- 30+ years of software development
- 25 years at Nokia
- Leading Linux OS development for Nokia Radio Cloud Products
- Responsible for software security vulnerability corrections
- PhD student at FI MUNI



Agenda

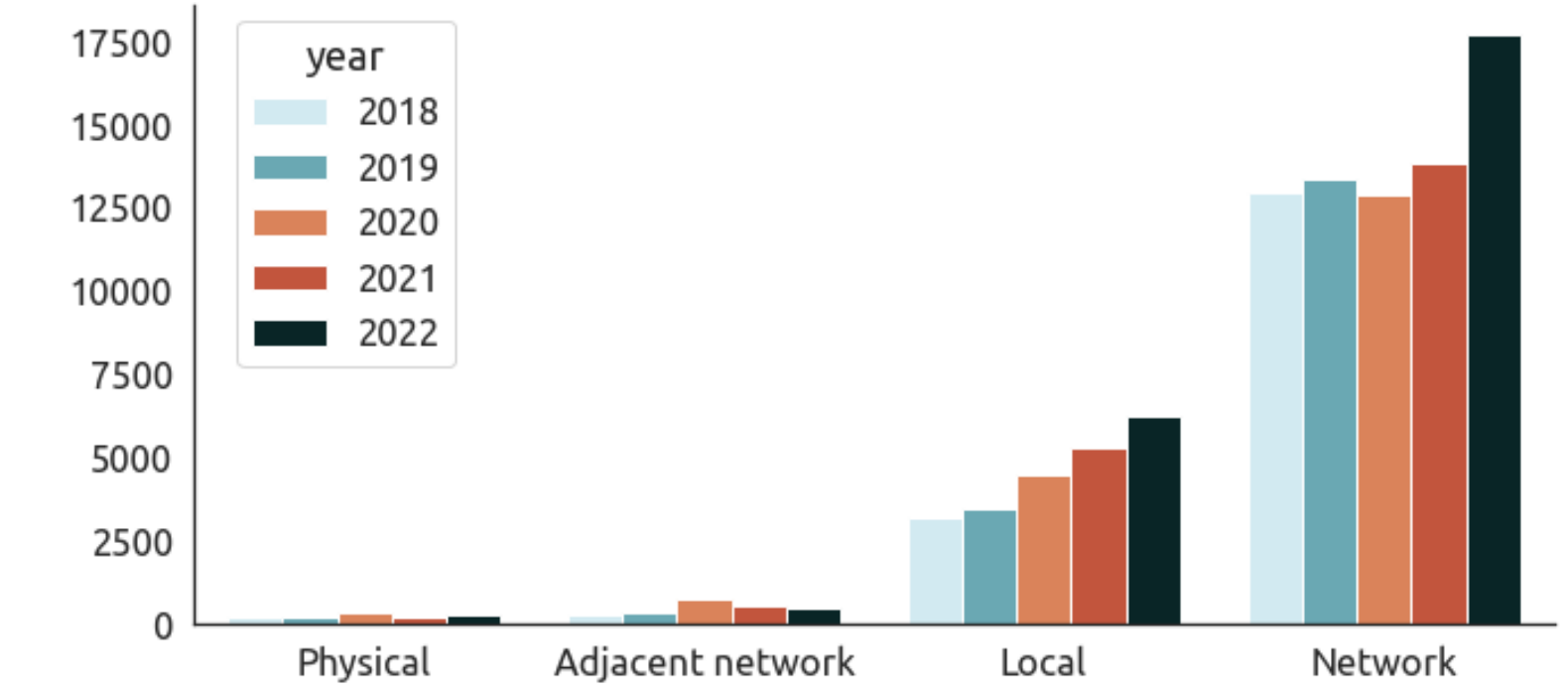
- Software security vulnerabilities
- Life cycle of a vulnerability
- Vulnerabilities in large scale software systems
- Examples

Generated by Adobe Firefly
Prompt: agenda for software vulnerability presentation

So how many software vulnerabilities are discovered per year?

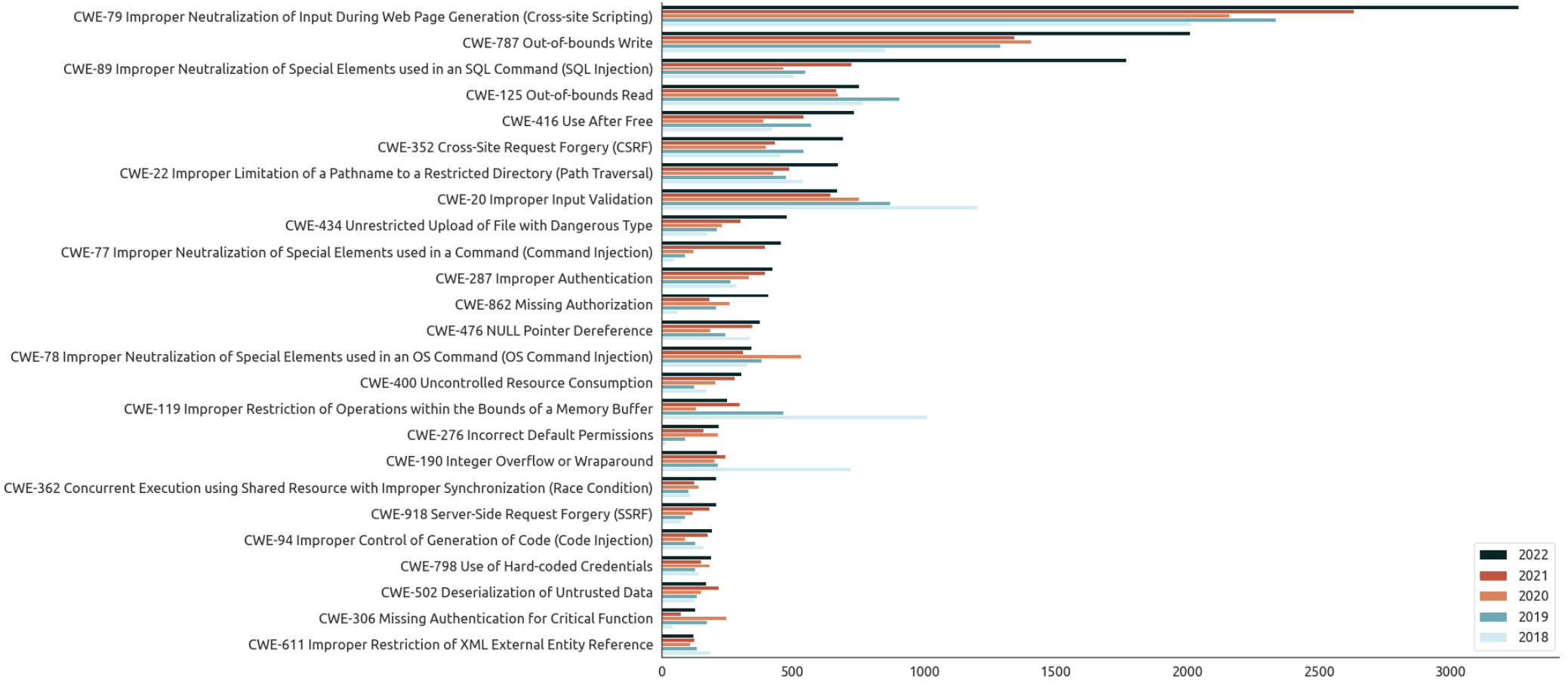
26 448 (2022)

https://bit.ly/3SmnQrz



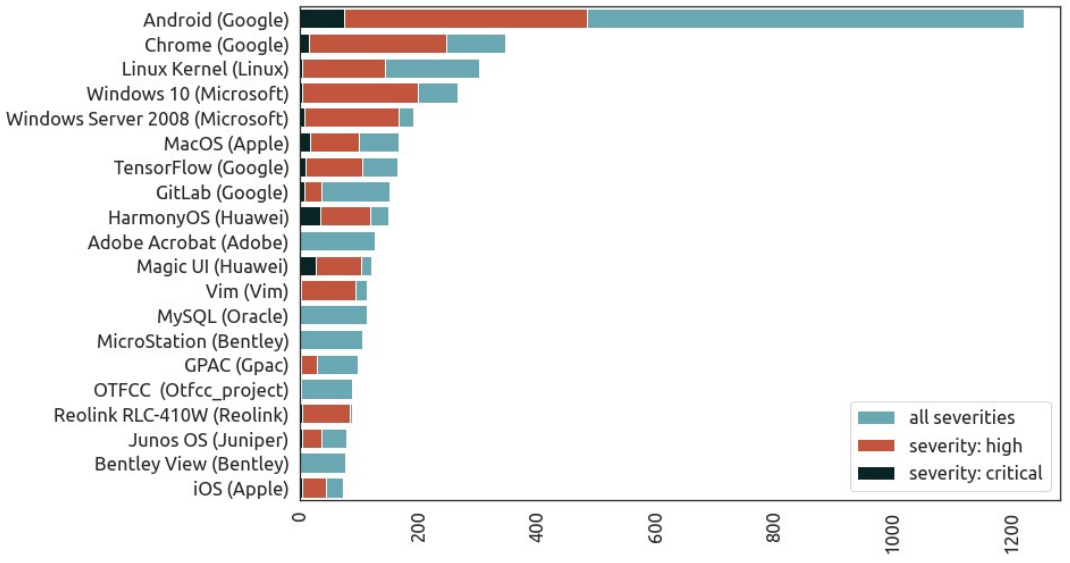
Graphic: Nick Sexton for The Stack. Source: nvd.nvist.gov

https://bit.ly/3SmnQrz

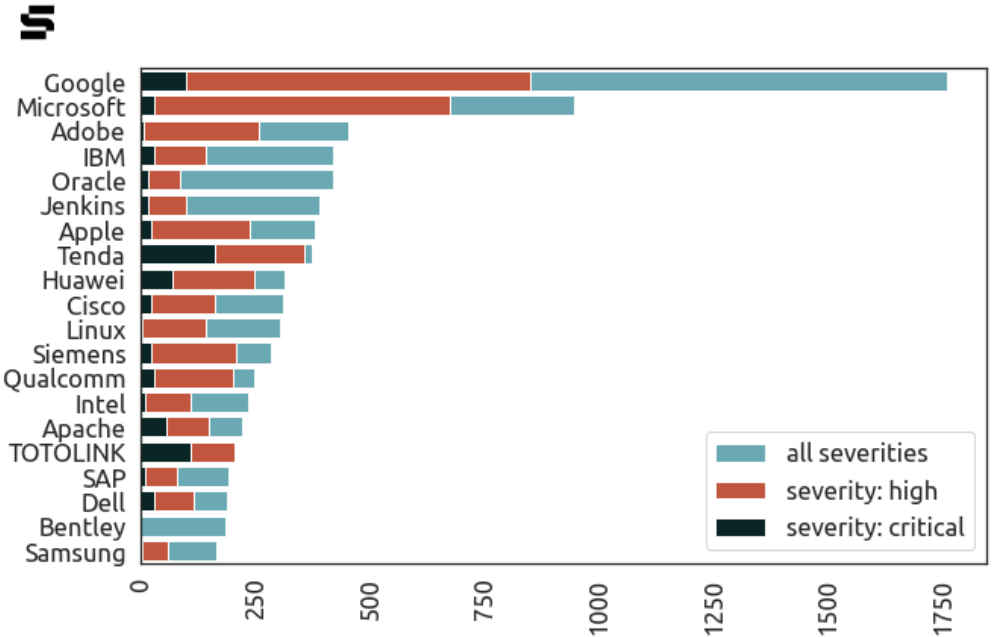


Graphic: Nick Sexton for The Stack. Source: nvd.nvist.gov

https://bit.ly/3SmnQrz



Graphic: Nick Sexton for The Stack. Source: nvd.nvist.gov



Graphic: Nick Sexton for The Stack. Source: nvd.nvist.gov

https://bit.ly/3SmnQrz

What are software security vulnerabilities?

https://bit.ly/3SpTnZF

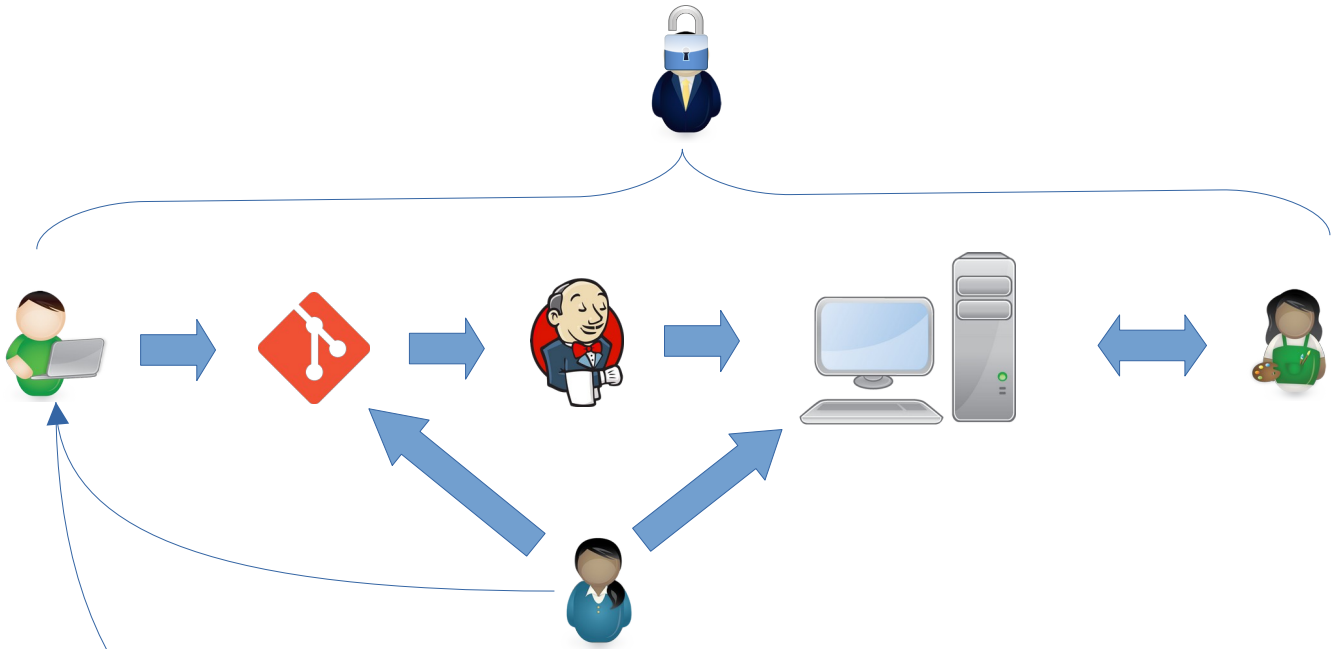
Software bugs affecting:

- **Confidentiality**
- **Integrity**
- **Availability**

Terminology

- **CVE** – Common Vulnerabilities and Exposures
- **CVSS** – Common Vulnerability Scoring System
- **CWE** – Common Weakness Enumeration

Life of a security vulnerability



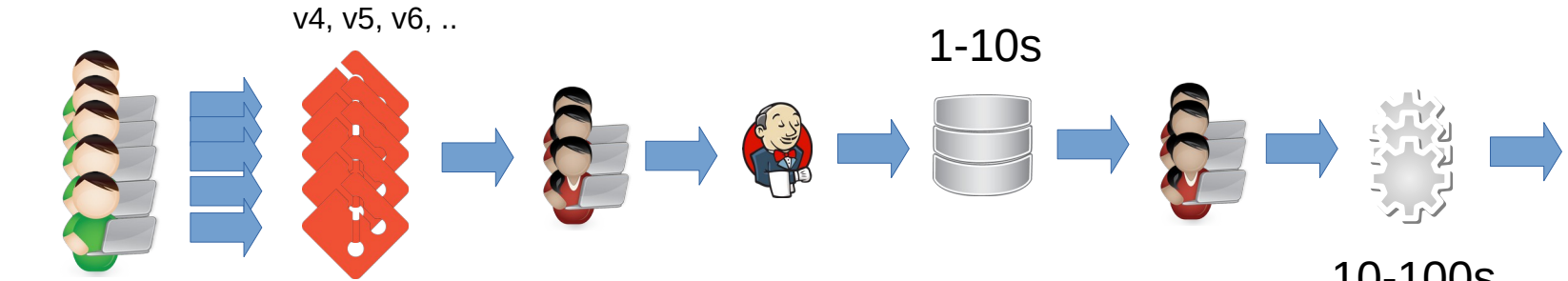
Programmer

Security expert

User

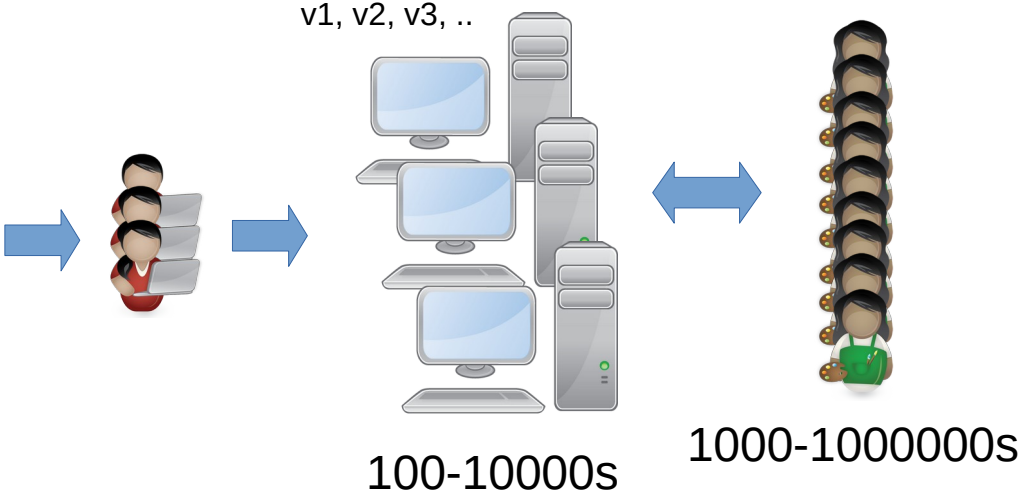
Cracker

Reality of large scale software system



Security Bug Generated by Adobe Firefly

100-1000s



Traceability
Scanning
Accuracy
Automation

Generated by Adobe Firefly

Traceability

SPDX

The Software Package Data Exchange

Open Vulnerability and Assessment Language

OVAL

Generated by Adobe Firefly
Prompt: software list of packages

Dangers of EOLs

No-one knows what bugs are in EOL software ...

... except for malicious attackers

Generated by Adobe Firefly
Prompt: unknown; dangerous; end of life; software; obsolete; old

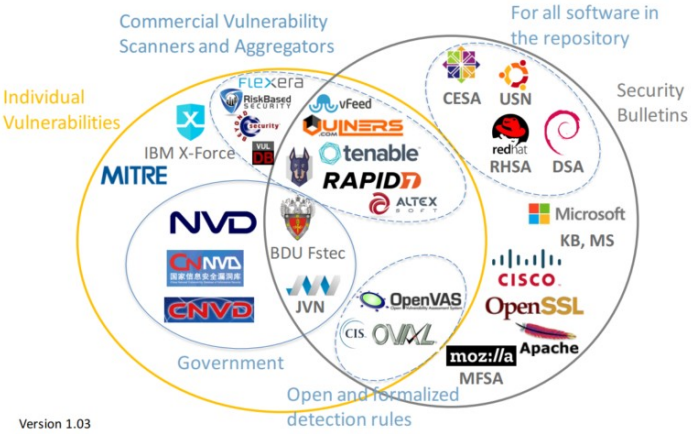
Scanning

- **Tools**
  - Trivy
  - Anchore
  - Clair
  - Grype

anchore

- **Databases**
  - cve.org
  - VulDB
  - NVD
  - OVAL

- **When**
  - Continuously



https://bit.ly/40nrVOm

- **Where**
  - Delivery chain
  - Production

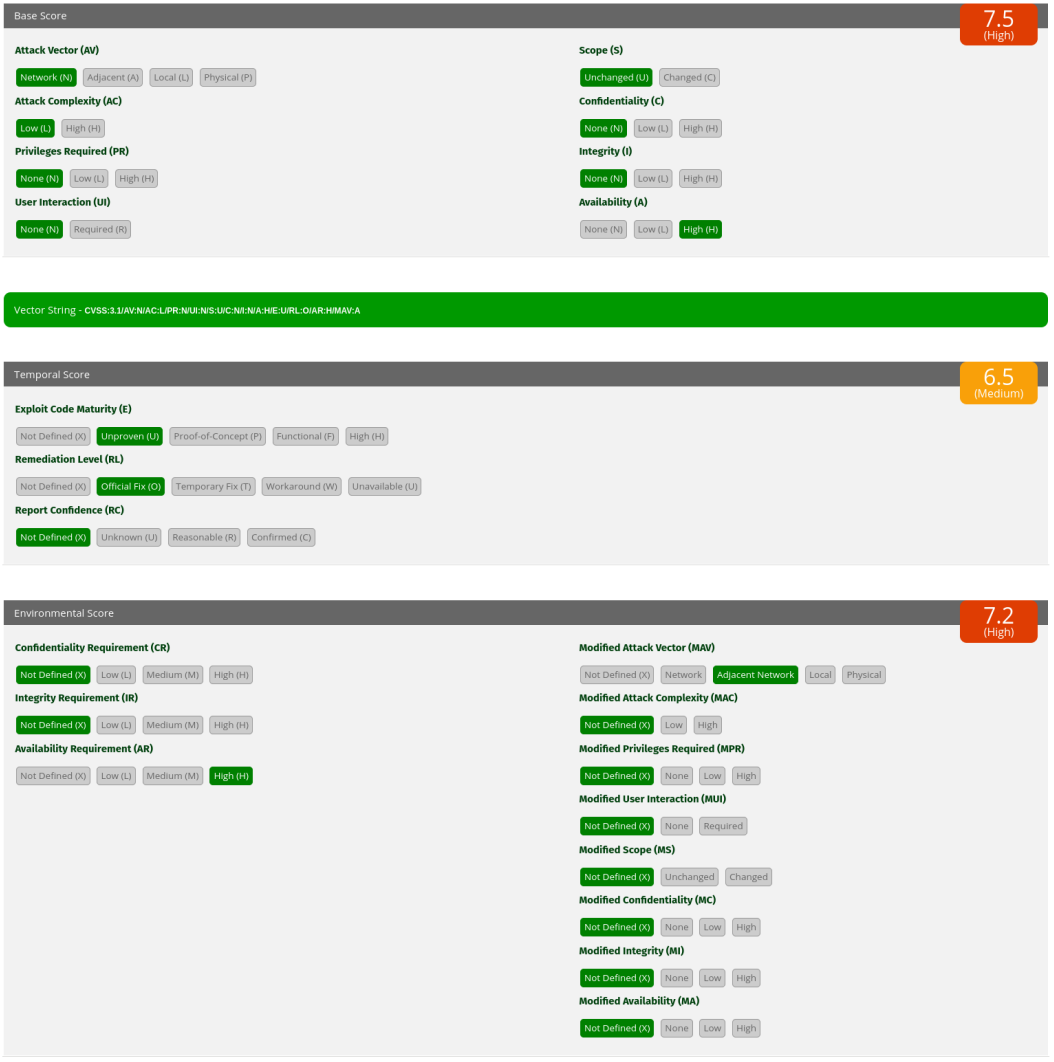
CYBERSECURITY RISK LEVELS

CVE SCORE V3.1

Severity	Base Score
No Risk	0
Low Risk	0.1-3.9
Medium Risk	4.0-6.9
High Risk	7.0-8.9
Critical Risk	9.0-10.0

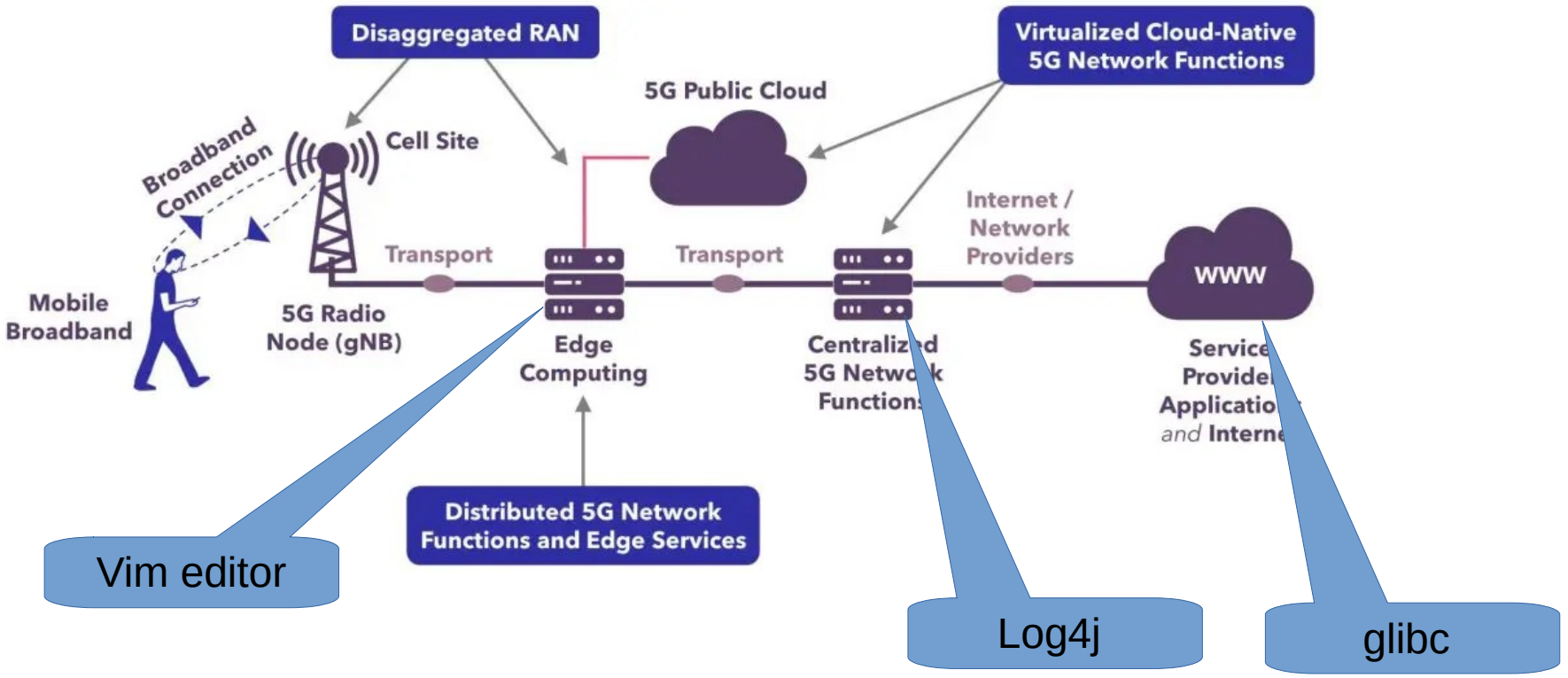
https://bit.ly/3SlECXG

Vulnerability assessment



https://bit.ly/3MkC7RR

Importance of Environmental setup

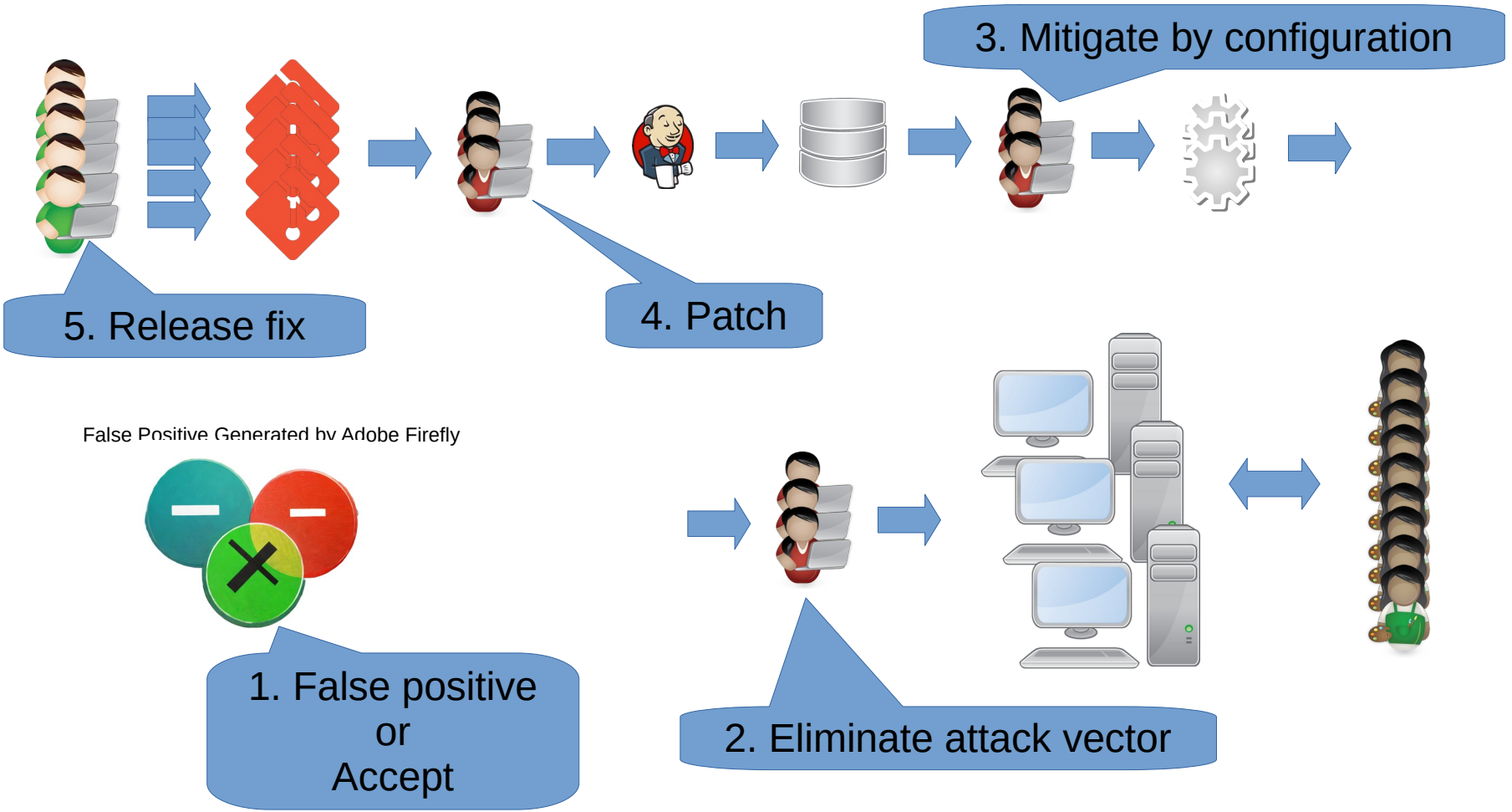


Remediation SLA – Service Level Agreement

Example

Low	300 days
Medium	30 days
High	5 days
Critical	2 days

Remediation – some of the options



CVE-2023-1355

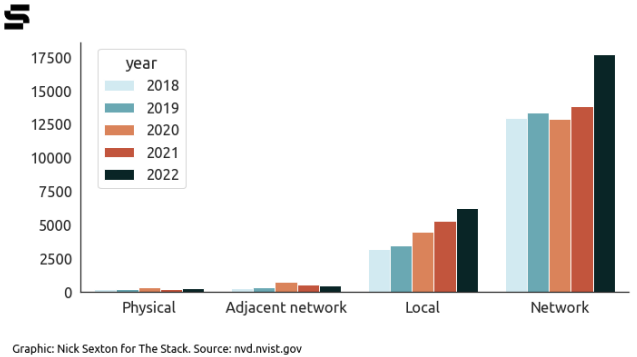
NULL Pointer Dereference in vim/vim

CVE-2023-4911

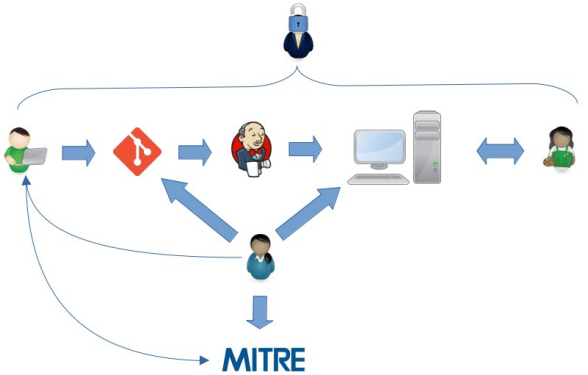
Buffer overflow in ld.so leading to privilege escalation

CVE-2021-44228
Log4Shell

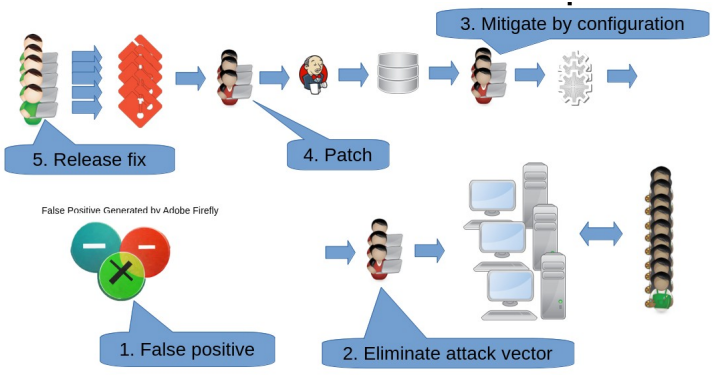
Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints

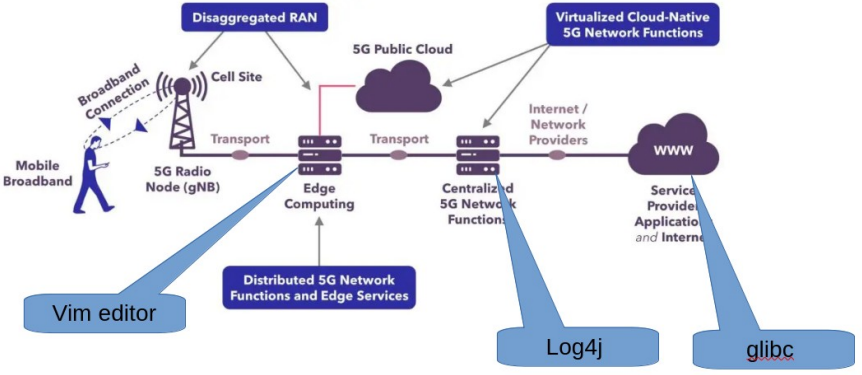


Graphic: Nick Sexton for The Stack. Source: nvd.nvist.gov



26 448





Links

- https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/AR:H/MAV:N/MAC:H
- https://www.cve.org/CVERecord?id=CVE-2023-1355
- https://nvd.nist.gov/vuln/detail/CVE-2023-1355
- https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2023-1355&vector=AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H&version=3.0&source=huntr.dev
- https://access.redhat.com/security/cve/cve-2023-1355
- https://security-tracker.debian.org/tracker/CVE-2023-1355
- https://www.cve.org/CVERecord?id=CVE-2023-4911
- https://nvd.nist.gov/vuln/detail/CVE-2023-4911
- https://access.redhat.com/security/cve/cve-2023-4911
- https://security-tracker.debian.org/tracker/CVE-2023-4911
- https://www.cve.org/CVERecord?id=CVE-2021-44228
- https://nvd.nist.gov/vuln/detail/CVE-2021-44228
- https://access.redhat.com/security/cve/cve-2021-44228
- https://security-tracker.debian.org/tracker/CVE-2021-44228