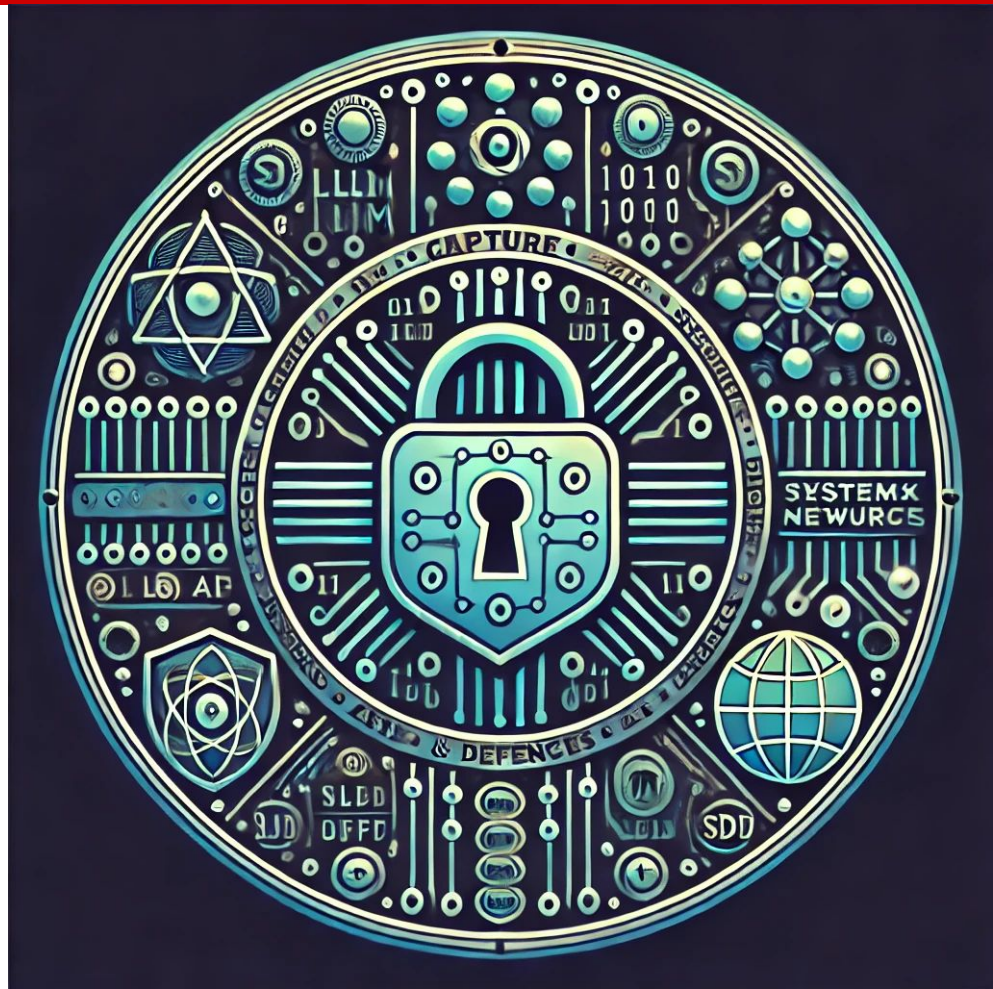
CSC-537 Systems Attacks and Defenses

Software Composition Analysis (SCA) & Security

Alexandros Kapravelos
akaprav@ncsu.edu



Deliverables

- **Challenge idea**: February 7
- **Challenge + PoC**: ~~February 21~~ February 28
- **Unit test/Code tranf/Prompt fix** for your own challenges: March 7
  - Test your challenges with Gemini 2.0 Flash for now

Attacking other teams:

- **Code tranf/Prompt fix** for other team challenges: March 21
- **Final challenges** deliverable (based on feedback): March 28

Introduction to Software Composition Analysis

What is Software Composition Analysis (SCA)?

- Automated identification of open-source components
- Evaluates:
  - Security vulnerabilities
  - License compliance
  - Code quality
- Typically integrated into development lifecycle
- Facilitates early detection of risks in software projects

Importance of SCA

- 70-90% of any given piece of modern software relies on open-source (via Linux Foundation)
- Enables faster development cycles
- Reduces redundant effort through reuse
- Potentially introduces security risks
- Allows proactive security management

Common Security Risks in OSS

- Known vulnerabilities in public databases
- Outdated or unmaintained packages
- Malicious code injection into packages
- Dependency confusion (typosquatting)
- Extensive dependency graphs increasing risk exposure

Real-World Case Studies

Log4Shell Vulnerability (2021)

- CVE-2021-44228, Log4j vulnerability
- Allowed remote code execution (RCE) through Java Naming and Directory Interface (JNDI) injection
  - Attackers can include malicious JNDI lookups in logged messages
  - Vulnerable Log4j versions automatically execute code downloaded through these lookups
  - This allows hackers to run arbitrary Java code on affected systems, potentially gaining full control
- Exploited via malicious log entries
- Global impact, widespread exploitation
- Maximum CVSS severity rating (10)

Impact of Log4Shell

- Potential impact on millions of systems
- Global patching efforts were massive
- Prompted security awareness shift globally
- Demonstrated OSS dependency security risks
- Increased adoption of automated security checks

Case Study: xz Backdoor Attack (2024)

- Compromise of popular compression library
- Malicious maintainer inserted SSH backdoor
- Early discovery prevented widespread harm
- Could have affected millions of Linux devices
- Led to review of OSS security policies

Other High-Profile Attacks

SolarWinds Orion (2020)

- Nation-state espionage via trusted software update
- Over 18,000 affected organizations

UA-Parser-JS (NPM) compromise in 2021

- Injected crypto-mining malware
- Over 8 million weekly downloads affected briefly

Practical Demonstrations

OWASP Dependency-Check

- Open-source vulnerability scanner
- Supports Java, Python, JavaScript, and more
- Integrates into build processes (CI/CD)
- Generates detailed vulnerability reports
- Uses NVD database to identify CVEs

Demo: k Usage

- Setting
> brew up k
- Runnin
> depende
- Review
- Integra
- Unders

Summary

Display: Showing Vulnerable Dependencies (click to show all)

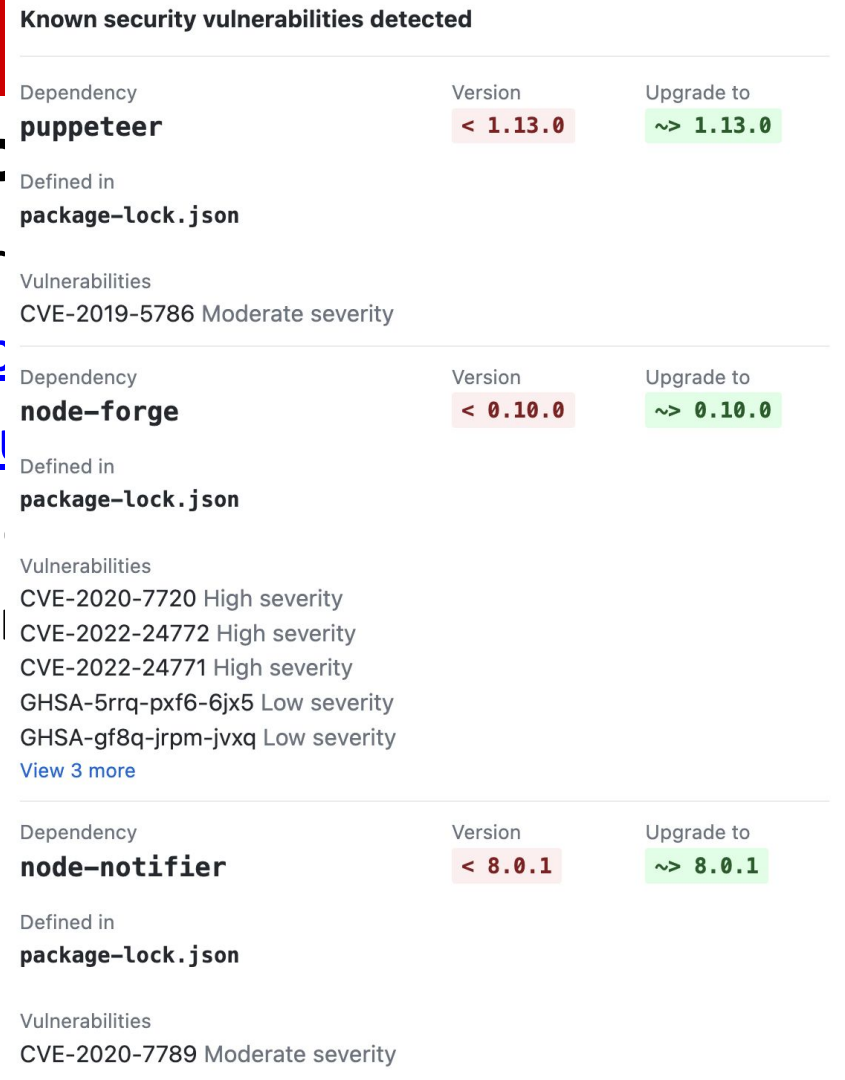
Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
ansi-regex:4.1.0	cpe:2.3:a:ansi-regex_project:ansi-regex:4.1.0:*:*:*:*:*:*:*	pkg:npm/ansi-regex@4.1.0	HIGH	2	Highest	10
body-parser:1.18.3		pkg:npm/body-parser@1.18.3	HIGH	2		7
cookie:0.3.1		pkg:npm/cookie@0.3.1	MEDIUM	1		9
cookie:0.4.0		pkg:npm/cookie@0.4.0	MEDIUM	2		9
cross-spawn:3.0.1		pkg:npm/cross-spawn@3.0.1	HIGH	2		10
ejs:2.6.2	cpe:2.3:a:ejs:ejs:2.6.2:*:*:*:*:*:*:*	pkg:npm/ejs@2.6.2	CRITICAL	4	Highest	10
express:4.16.4		pkg:npm/express@4.16.4	HIGH	6		9
flat:5.0.0	cpe:2.3:a:flat_project:flat:5.0.0:*:*:*:*:*:*:*	pkg:npm/flat@5.0.0	CRITICAL	2	Highest	10
helper.js		pkg:javascript/lodash@1.0.1	CRITICAL	6		3
hosted-git-info:2.8.8		pkg:npm/hosted-git-info@2.8.8	MEDIUM	2		10
json-schema:0.2.3	cpe:2.3:a:json-schema_project:json-schema:0.2.3:*:*:*:*:*:*:*	pkg:npm/json-schema@0.2.3	CRITICAL	2	Highest	10
lodash.js		pkg:javascript/lodash@4.17.19	HIGH	2		3
lodash.min.js		pkg:javascript/lodash@4.17.19	HIGH	2		3
lodash:4.17.19	cpe:2.3:a:lodash:lodash:4.17.19:*:*:*:*:*:*:*	pkg:npm/lodash@4.17.19	HIGH	5	Highest	9
minimatch:3.0.4	cpe:2.3:a:minimatch_project:minimatch:3.0.4:*:*:*:*:*:*:*	pkg:npm/minimatch@3.0.4	HIGH	2	Highest	10
minimist:1.2.5	cpe:2.3:a:substack:minimist:1.2.5:*:*:*:*:*:*:*	pkg:npm/minimist@1.2.5	CRITICAL	2	Highest	10
moment.js		pkg:javascript/moment.js@2.20.1	HIGH	2		3
node-sass:4.14.1	cpe:2.3:a:sass-lang:node-sass:4.14.1:*:*:*:*:*:*:*	pkg:npm/node-sass@4.14.1	MEDIUM	2	Highest	10
path-parse:1.0.6	cpe:2.3:a:path-parse_project:path-parse:1.0.6:*:*:*:*:*:*:*	pkg:npm/path-parse@1.0.6	HIGH	2	Highest	9
path-to-regexp:0.1.7		pkg:npm/path-to-regexp@0.1.7	HIGH	3		7
qs:6.5.2	cpe:2.3:a:qs_project:qs:6.5.2:*:*:*:*:*:*:*	pkg:npm/qs@6.5.2	HIGH	2	Highest	7
request:2.88.2	cpe:2.3:a:request_project:request:2.88.2:*:*:*:*:*:*:*	pkg:npm/request@2.88.2	MEDIUM	2	Highest	9
scss-tokenizer:0.2.3	cpe:2.3:a:scss-tokenizer_project:scss-tokenizer:0.2.3:*:*:*:*:*:*:*	pkg:npm/scss-tokenizer@0.2.3	HIGH	2	Highest	8
semver:5.3.0		pkg:npm/semver@5.3.0	HIGH	2		7
semver:5.7.1		pkg:npm/semver@5.7.1	HIGH	1		7
send:0.16.2	cpe:2.3:a:send_project:send:0.16.2:*:*:*:*:*:*:*	pkg:npm/send@0.16.2	MEDIUM	2	Highest	9
serve-static:1.13.2	cpe:2.3:a:serve-static_project:serve-static:1.13.2:*:*:*:*:*:*:*	pkg:npm/serve-static@1.13.2	MEDIUM	2	Highest	9
tar:2.2.2	cpe:2.3:a:tar_project:tar:2.2.2:*:*:*:*:*:*:*	pkg:npm/tar@2.2.2	HIGH	6	Highest	10
tough-cookie:2.5.0	cpe:2.3:a:salesforce:tough-cookie:2.5.0:*:*:*:*:*:*:*	pkg:npm/tough-cookie@2.5.0	CRITICAL	2	Highest	9
trim-newlines:1.0.0	cpe:2.3:a:trim-newlines_project:trim-newlines:1.0.0:*:*:*:*:*:*:*	pkg:npm/trim-newlines@1.0.0	HIGH	2	Highest	10
underscore-min.js		pkg:javascript/underscore.js@1.6.0	HIGH	1		3
underscore.js		pkg:javascript/underscore.js@1.6.0	HIGH	1		3
underscore:1.6.0	cpe:2.3:a:underscorejs:underscore:1.6.0:*:*:*:*:*:*:*	pkg:npm/underscore@1.6.0	CRITICAL	2	Highest	9
y18n:4.0.0	cpe:2.3:a:y18n_project:y18n:4.0.0:*:*:*:*:*:*:*	pkg:npm/y18n@4.0.0	CRITICAL	2	Highest	9

GitHub Dependabot Overview

- Automatic dependency monitoring tool
- Creates automated security patches via PRs
- Customizable alerts and update schedules
- Easy integration into GitHub repositories
- Enables proactive vulnerability management

Demo: Co pendabot

- Enabling in r
- Creating dep
- Reviewing pu
- Resolving se
- Configuring ates



Known security vulnerabilities detected

Dependency **puppeteer** Version `< 1.13.0` Upgrade to `~> 1.13.0`

Defined in **package-lock.json**

Vulnerabilities
CVE-2019-5786 Moderate severity

Dependency **node-forge** Version `< 0.10.0` Upgrade to `~> 0.10.0`

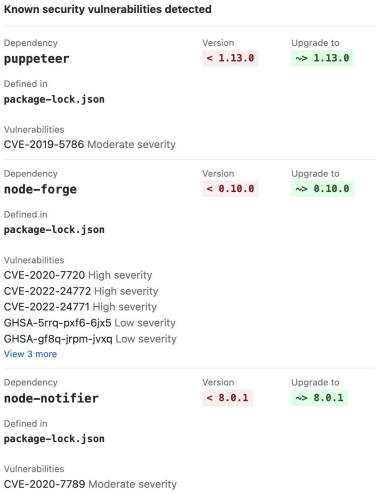
Defined in **package-lock.json**

Vulnerabilities
CVE-2020-7720 High severity
CVE-2022-24772 High severity
CVE-2022-24771 High severity
GHSA-5rrq-pxf6-6jx5 Low severity
GHSA-gf8q-jrpm-jvxq Low severity
View 3 more

Dependency **node-notifier** Version `< 8.0.1` Upgrade to `~> 8.0.1`

Defined in **package-lock.json**

Vulnerabilities
CVE-2020-7789 Moderate severity



Known security vulnerabilities detected

Dependency	Version	Upgrade to
puppeteer	`< 1.13.0`	`~> 1.13.0`

Defined in
package-lock.json

Vulnerabilities
CVE-2019-5786 Moderate severity

Dependency	Version	Upgrade to
node-forge	`< 0.10.0`	`~> 0.10.0`

Defined in
package-lock.json

Vulnerabilities
CVE-2020-7720 High severity
CVE-2022-24772 High severity
CVE-2022-24771 High severity
GHSA-5rrq-pxf6-6jx5 Low severity
GHSA-gf8q-jrpm-jvxq Low severity
View 3 more

Dependency	Version	Upgrade to
node-notifier	`< 8.0.1`	`~> 8.0.1`

Defined in
package-lock.json

Vulnerabilities
CVE-2020-7789 Moderate severity

Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
ansi-regex:4.1.0	cpe:2.3:a:ansi-regex_project:ansi-regex:4.1.0:*:*:*:*:*:*:*	pkg:npm/ansi-regex@4.1.0	HIGH	2	Highest	10
body-parser:1.18.3		pkg:npm/body-parser@1.18.3	HIGH	2		7
cookie:0.3.1		pkg:npm/cookie@0.3.1	MEDIUM	1		9
cookie:0.4.0		pkg:npm/cookie@0.4.0	MEDIUM	2		9
cross-spawn:3.0.1		pkg:npm/cross-spawn@3.0.1	HIGH	2		10
ejs:2.6.2	cpe:2.3:a:ejs:ejs:2.6.2:*:*:*:*:*:*:*	pkg:npm/ejs@2.6.2	CRITICAL	4	Highest	10
express:4.16.4		pkg:npm/express@4.16.4	HIGH	6		9
flat:5.0.0	cpe:2.3:a:flat_project:flat:5.0.0:*:*:*:*:*:*:*	pkg:npm/flat@5.0.0	CRITICAL	2	Highest	10
heber.js		pkg:javascript/lodash@1.0.1	CRITICAL	6		3
hosted-git-info:2.8.8		pkg:npm/hosted-git-info@2.8.8	MEDIUM	2		10
json-schema:0.2.3	cpe:2.3:a:json-schema_project:json-schema:0.2.3:*:*:*:*:*:*:*	pkg:npm/json-schema@0.2.3	CRITICAL	2	Highest	10
lodash.js		pkg:javascript/lodash@4.17.19	HIGH	2		3
lodash.min.js		pkg:javascript/lodash@4.17.19	HIGH	2		3
lodash:4.17.19	cpe:2.3:a:lodash:lodash:4.17.19:*:*:*:*:*:*:*	pkg:npm/lodash@4.17.19	HIGH	5	Highest	9
minimatch:3.0.4	cpe:2.3:a:minimatch_project:minimatch:3.0.4:*:*:*:*:*:*:*	pkg:npm/minimatch@3.0.4	HIGH	2	Highest	10
minimist:1.2.5	cpe:2.3:a:substack:minimist:1.2.5:*:*:*:*:*:*:*	pkg:npm/minimist@1.2.5	CRITICAL	2	Highest	10
moment.js		pkg:javascript/moment.js@2.20.1	HIGH	2		3
node-sass:4.14.1	cpe:2.3:a:sass-lang:node-sass:4.14.1:*:*:*:*:*:*:*	pkg:npm/node-sass@4.14.1	MEDIUM	2	Highest	10
path-parse:1.0.6	cpe:2.3:a:path-parse_project:path-parse:1.0.6:*:*:*:*:*:*:*	pkg:npm/path-parse@1.0.6	HIGH	2	Highest	9
path-to-regexp:0.1.7		pkg:npm/path-to-regexp@0.1.7	HIGH	3		7
qs:6.5.2	cpe:2.3:a:qs_project:qs:6.5.2:*:*:*:*:*:*:*	pkg:npm/qs@6.5.2	HIGH	2	Highest	7
request:2.88.2	cpe:2.3:a:request_project:request:2.88.2:*:*:*:*:*:*:*	pkg:npm/request@2.88.2	MEDIUM	2	Highest	9
scss-tokenizer:0.2.3	cpe:2.3:a:scss-tokenizer_project:scss-tokenizer:0.2.3:*:*:*:*:*:*:*	pkg:npm/scss-tokenizer@0.2.3	HIGH	2	Highest	8
semver:5.3.0		pkg:npm/semver@5.3.0	HIGH	2		7
semver:5.7.1		pkg:npm/semver@5.7.1	HIGH	1		7
send:0.16.2	cpe:2.3:a:send_project:send:0.16.2:*:*:*:*:*:*:*	pkg:npm/send@0.16.2	MEDIUM	2	Highest	9
serve-static:1.13.2	cpe:2.3:a:serve-static_project:serve-static:1.13.2:*:*:*:*:*:*:*	pkg:npm/serve-static@1.13.2	MEDIUM	2	Highest	9
tar:2.2.2	cpe:2.3:a:tar_project:tar:2.2.2:*:*:*:*:*:*:*	pkg:npm/tar@2.2.2	HIGH	6	Highest	10
tough-cookie:2.5.0	cpe:2.3:a:salesforce:tough-cookie:2.5.0:*:*:*:*:*:*:*	pkg:npm/tough-cookie@2.5.0	CRITICAL	2	Highest	9
trim-newlines:1.0.0	cpe:2.3:a:trim-newlines_project:trim-newlines:1.0.0:*:*:*:*:*:*:*	pkg:npm/trim-newlines@1.0.0	HIGH	2	Highest	10
underscore-min.js		pkg:javascript/underscore.js@1.6.0	HIGH	1		3
underscore.js		pkg:javascript/underscore.js@1.6.0	HIGH	1		3
underscore:1.6.0	cpe:2.3:a:underscorejs:underscore:1.6.0:*:*:*:*:*:*:*	pkg:npm/underscore@1.6.0	CRITICAL	2	Highest	9
y18n:4.0.0	cpe:2.3:a:y18n_project:y18n:4.0.0:*:*:*:*:*:*:*	pkg:npm/y18n@4.0.0	CRITICAL	2	Highest	9

Discussion: how do you handle alerts?

Exploiting a Vulnerable Package

- Demonstration of exploitation process
- Highlighting ease of exploiting known issues
- Importance of timely patching
- Illustration using intentionally vulnerable package
- Practical attacker perspective demonstration

Securing the Software Supply Chain

Defense-in-Depth Strategy

- Layered security to reduce risk
- Incorporate automated checks in CI/CD pipelines
- Continuous vulnerability scanning
- Regular dependency audits and updates
- Comprehensive education and awareness training

Best Practices for Secure OSS

- Regular updates and proactive patching
- Continuous monitoring for new vulnerabilities
- Assessment of OSS project health
- Restricting dependencies to minimize risks
- Internal security policy and clear documentation

Software Bill of Materials (SBOM)

- Comprehensive list of software dependencies
- Facilitates rapid response to security alerts
- Industry-standard practice and regulatory compliance
- Key to transparency in software supply chains
- Streamlines vulnerability management and remediation

Cryptographic Integrity Checks

- Digital signatures and checksum validation
- Prevent tampering and ensure authenticity
- Standard recommendation for software security
- Part of holistic security approach

Key Takeaways

- SCA essential due to pervasive OSS usage
- High-profile vulnerabilities illustrate significant risk
- OWASP Dependency-Check and Dependabot critical for proactive security
- Implement regular updates, maintain SBOMs, manage dependencies rigorously
- Ongoing security vigilance and developer education vital