

Waiter, there's a CVE in my SOUP

Software Composition Analysis

Kevin Alcock - Director, Application Security

Thank You to Our Sponsors and Hosts!



Without them, this Conference couldn't happen.



A few definitions

- **A06:2021**
Vulnerable and Outdated Components
- **SOUP**
Software Of Unknown Provenance
- **CVE**
Common Vulnerabilities and Exposures
- **CWE**
Common Weakness Enumeration
- **CPE**
Common Platform Enumeration
- **CVSS**
Common Vulnerability Scoring System
- **NVD**
National Vulnerability Database
- **SCA**
Software Composition Analysis
- **KEV**
CISA's Known Exploited Vulnerabilities Catalog
- **SBOM**
Software Bill Of Materials



Look at CVE-2021-44228

CVE-2021-44228 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

<https://nvd.nist.gov/vuln/detail/cve-2021-44228>



Look at CVE-2021-44228

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score:

10.0 CRITICAL

Vector:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

<https://nvd.nist.gov/vuln/detail/cve-2021-44228>



Look at CVE-2021-44228

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score:

10.0 CRITICAL

Vector:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H



NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

<https://nvd.nist.gov/vuln/detail/cve-2021-44228>



Look at CVE-2021-44228

Vector	
Attack Vector (AV)	Network
Attack Complexity (AC)	Low
Privileges Required (PR)	None
User Interaction (UI)	None
Scope (S)	Changed
Confidentiality Impact (C):	High
Integrity Impact (I)	High
Availability Impact (A):	High

Vector:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

... strings and CVSS scores. We also display any CVSS

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis.

The CNA has not provided a score within the CVE List.

<https://nvd.nist.gov/vuln/detail/cve-2021-44228>







Look at CVE-2021-44228

This CVE is in CISA's Known Exploited Vulnerabilities Catalog

Reference CISA's BOD 22-01 and Known Exploited Vulnerabilities Catalog for further guidance and requirements.

Vulnerability Name	Date Added	Due Date	Required Action
Apache Log4j2 Remote Code Execution Vulnerability	12/10/2021	12/24/2021	For all affected software assets for which updates exist, the only acceptable remediation actions are: 1) Apply updates; OR 2) remove affected assets from agency networks. Temporary mitigations using one of the measures provided at https://www.cisa.gov/uscert/ed-22-02-apache-log4j-recommended-mitigation-measures are only acceptable until updates are available.

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-917	Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression La	 NIST
CWE-400	Uncontrolled Resource Consumption	 Apache Software Foundation
CWE-502	Deserialization of Untrusted Data	 Apache Software Foundation
CWE-20	Improper Input Validation	 Apache Software Foundation

<https://nvd.nist.gov/vuln/detail/cve-2021-44228>

What does Software Composition Analysis give us

- Identify vulnerable dependencies
- Monitor for new vulnerabilities
- License compliance management
- Automated remediation strategies



Some SCA tools

- Black Duck - Synopsys
- Checkmarx
- GitLab Ultimate
- Github Dependabot
- Mend.io - Formally WhiteSource
- Snyk SCA
- Sonartype
- Trivy - Aqua Security





OWASP to the rescue

Dependency Check

Software Composition Analysis (SCA) tool that attempts to detect publicly disclosed vulnerabilities contained within a project's dependencies.

Leader: Jeremy Long

<https://owasp.org/www-project-dependency-check/>

Dependency Track

Component Analysis platform that allows organizations to identify and reduce risk in the software supply chain.

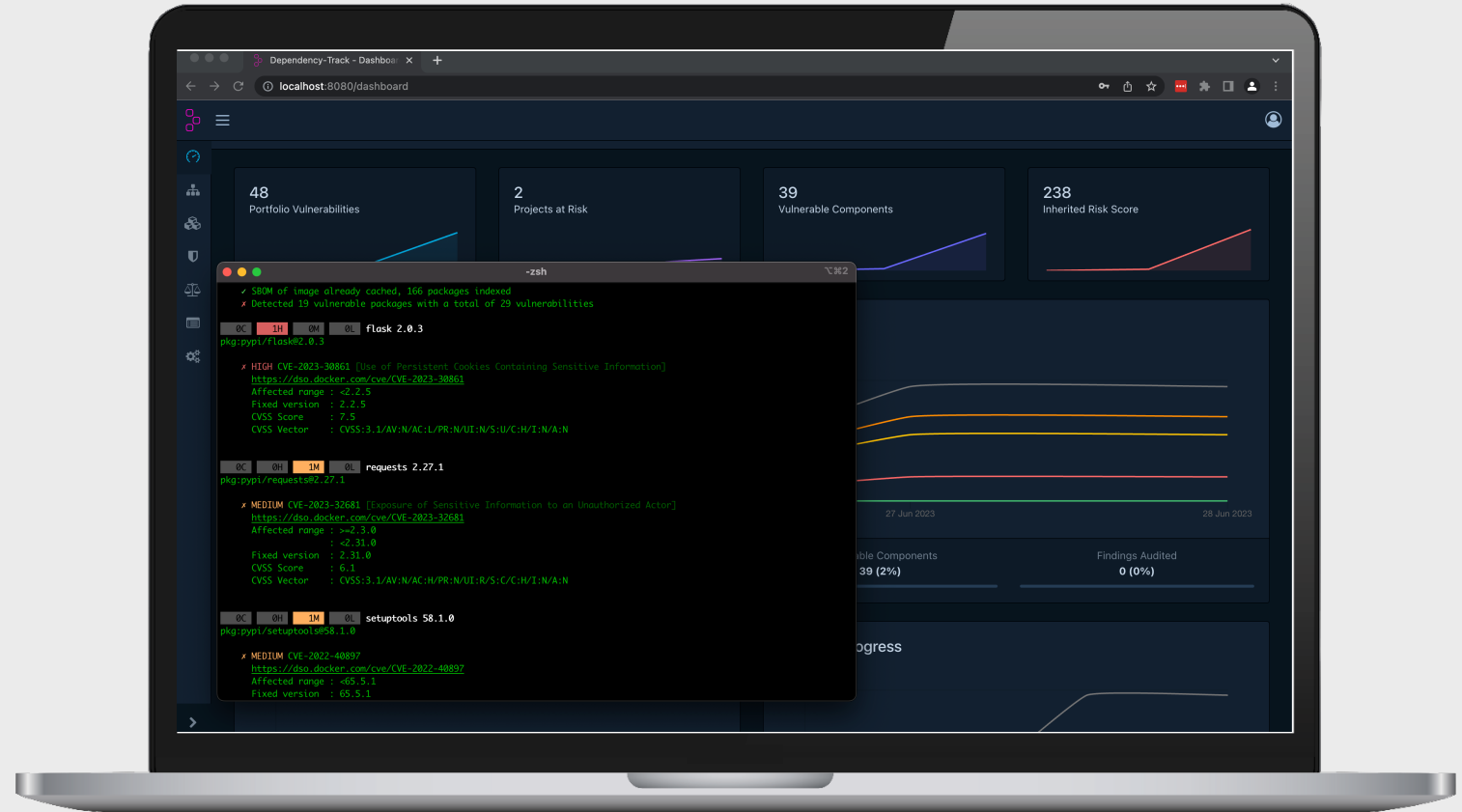
Leaders: Steve Springett & Niklas Düster

<https://dependencytrack.org/>



Demo time

- Dependency check
- Dependency track
- And Containers



Final Words

- Don't worry about the noise, concentrate on the signal
- Integrate SCA tooling into your build pipeline
- Not all CVE's are created equal
- If can, live on the edge
- If you can't, mitigate and monitor
- Block new dependencies with "Critical" vulnerabilities
- Automate PR's when you have good automated testing
- Create SBOM's for each release

- Thank you 🙌

