TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-interner Workshop

28.06.2023, Berlin

Software Bill of Materials (SBOM)

Oliver Dehning

Eine Meldung im Dezember 2021 …

… über eine kritische Zero-Day-Sicherheitslücke namens Log4Shell in der weitverbreiteten Java-Logging-Bibliothek Log4j können Angreifer beliebigen Code ausführen lassen. Betroffen sind etwa Dienste von Apple, Twitter, Steam, Amazon und vermutlich sehr viele kleinere Angebote. Es gibt Proof-of-Concept-Code, der das Ausnutzen der Lücke demonstriert und auch bereits erste Angriffe. Seit Kurzem steht ein Quellcode-Update des Apache-Projekts bereit; Admins sollten dringend aktiv werden …

Apache Log4J

- Java Bibliothek – Logging Framework
- Einsatz in einer unübersehbaren Zahl von Anwendungen, häufig im Backend
- Sicherheitslücke ermöglicht Ausführung praktisch beliebigen Codes
- Betroffene Anbieter: Apache, Atlassian, Cisco, Cyberark, Elastic, Fortinet, F-Secure, IBM, IGEL, Jitsi, Juniper, McAfee, Netflix, RSA, SAP, SolarWinds, Sophos, Splunk, Teamviewer, TrendMicro, VMWare, …
  (https://github.com/NCSC-NL/log4shell/tree/main/software)
- Entdeckt und behoben im Dezember 2021

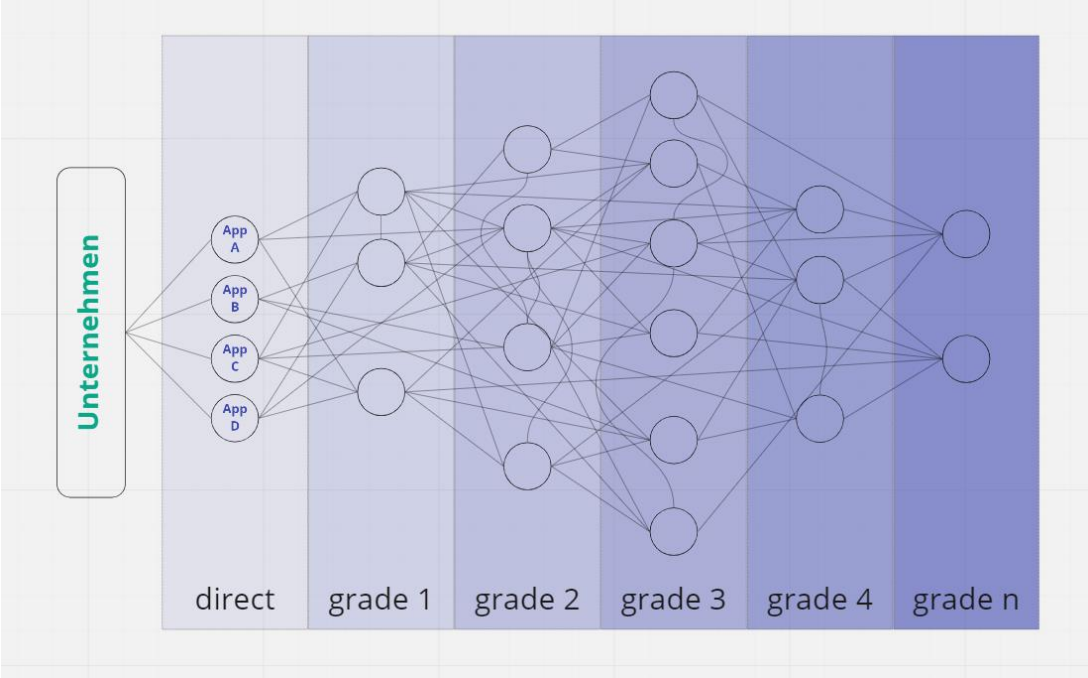
Die zentrale Frage in solchen Fällen

… es gibt Meldungen über eine neue Lücke in einer zentralen Software-Bibliothek / einem zentralen Dienst.

Sind wir betroffen?

Das eigentliche Problem

- Software und (allgemeiner) IT-Dienste bestehen aus unzählig vielen aufeinander aufbauenden Komponenten.
- Aufbau und Inhalt sind i.d.R. mindestens für den Anwender vollkommen intransparent.



Transparenz schaffen

- Verständnis der Softwarezusammensetzung
- Identifikation von Abhängigkeiten
- Bewertung von Risiken
- Verfolgung von Änderungen
- Bewertung von Schwachstellen

Software Bill of Materials

Software Bill of Materials (Software-Stückliste, SBOM):

- Formale und maschinenlesbare Metadaten, die ein Softwarepaket und seinen Inhalt eindeutig identifizieren
- Transparenz über die Komponenten einer Software-Lieferkette

SBOM: Standards (Datenformate):

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Software Package Data Exchange (SPDX)
  (ISO/IEC 5962:2021)
- Software Identification Tag (SWID)
  (ISO/IEC 19770-2:2015)
- CycloneDX
  (OWASP)

SBOM: Werkzeuge

- Erstellen von SBOMs während des Build-Prozesses
- Analysieren von Quellcode und Binärdateien (Container-Images), Erzeugen von SBOMs daraus
- SBOMs bearbeiten
- Anzeigen, Vergleichen, Importieren und Validieren von SBOMs in einem für Menschen lesbaren Format
- Zusammenführen und Übersetzen von SBOM-Inhalten von einem Format oder Dateityp in ein anderes
- Unterstützung der Verwendung von SBOM-Manipulationen in anderen Tools über APIs und Bibliotheken
- Integration mit bestehenden Tools wie Schwachstellen-Scannern und Tools zum Testen der Anwendungssicherheit
- Berichte und Analysen (Aufschluss über potenzielle Sicherheitsrisiken)

SBOM: Regulierung

- US Executive Order 14028 (Mai 2021)
  - Improve software supply chain security
  - The Commerce Department must publish minimum elements for a software bill of materials (SBOM) that traces the individual components that make up software.
  - https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- NIST Guidance for Cybersecurity Supply Chain Risk Management (Mai 2022)
  - Establish a governance capability for managing and monitoring components of embedded software to manage risk across the enterprise (e.g., SBOMs paired with criticality, vulnerability, threat, and exploitability to make this more automated).
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
- European Commission: Proposal for a Regulation on cybersecurity requirements for products with digital elements - Cyber resilience Act (15.9.2022)
  - "In order to facilitate vulnerability analysis, manufacturers should identify and document components contained in the products with digital elements, including by drawing up a software bill of materials."
  - "A software bill of materials can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, most notably it helps manufacturers and users to track known newly emerged vulnerabilities and risks."
- Plan: Verabschiedung 2024, wirksam ab 2026

Fragestellungen (Aufgaben für die AG Cloud Security)

- Welches Datenformat?
- Welche Werkzeuge stehen zur Verfügung? (Was fehlt?)
- BOM über Software hinaus (Hardware, Cloud-Services)?
- Authentisierung und Validierung?
- Dynamische Bereitstellung von SBOMs?
- Entwicklung gesetzlicher Anforderungen?
- Was sollten Anwender, Betreiber und ISVs in Bezug auf SBOMs tun?