Sicherheitslücken mit OWASP Dependency Check Plugin im Jenkins überwachen

Dr. André Janus

Mi. 10. Mai 2023

JUG Karlsruhe

jug-karlsruhe.de | twitter.com/@jugka

IT-Experten

Große Sorgen wegen Log4j-Schwachstelle

Stand: 13.12.2021 18:11 Uhr

Unternehmen und Behörden in Deutschland sind wegen möglicher Hackerangriffe in Habachtstellung. Am Wochenende hatte die IT-Sicherheitsbehörde BSI Alarmstufe Rot wegen einer Schwachstelle einer Server-Software ausgerufen. Sie rät nun dringend zu Updates.

Bei den IT-Sicherheitsexperten klingelten spätestens am Wochenende die Alarmglocken. Da hatte das Bundesamt für Sicherheit in der Informationstechnik BSI die höchste Warnstufe ausgesprochen. Es gebe eine extrem kritische Bedrohungslage hieß es aus Bonn: eine Schwachstelle in einer Java-Komponente namens Log4j.

Und die macht den Fachleuten auch zum Wochenstart immer noch größte Sorge, sagt BSI-Präsident Arne Schönbohm: "Es geht darum, dass wir auf der einen Seite gesehen haben, das Produkt wird überall eingesetzt in allen möglichen anderen Produkten. Es ist praktisch ein kleiner Bestandteil von einem übergeordneten Softwareprodukt. Das ist das eine Thema, also große Verbreitung. Das zweite Thema ist, dass es eine Schwachstelle ist, die sehr, sehr einfach auszunutzen ist." Noch wissen die Experten gar nicht, in wie vielen Anwendungen das gefährliche Softwaremodul steckt.

tagesschau live: BSI informiert über IT-Sicherheitslücke
13.12.2021 · 15:46 Uhr

Quelle: https://www.einfachvorlesen.de/geschichten/der-tag-dem-oma-das-internet-kaputt-gemacht-hat?bonus=toll

Agenda

- Software-Abhängigkeiten & Sicherheitslücken
  - Was? Warum? Wer? ...
  - CVE, CPE, CWE, CVSS

Agenda

- Software-Abhängigkeiten & Sicherheitslücken
  - Was? Warum? Wer? ...
  - CVE, CPE, CWE, CVSS
- OWASP Dependency Check
  - Sicherheitslücken in Software-Abhängigkeiten

Agenda

- Software-Abhängigkeiten & Sicherheitslücken
  - Was? Warum? Wer? ...
  - CVE, CPE, CWE, CVSS
- OWASP Dependency Check
  - Sicherheitslücken in Software-Abhängigkeiten
- OWASP Dependency Check Jenkins Plugin
  - Kontinuierliche Überwachung in CI

Software-Abhängigkeiten & Sicherheitslücken

- Warum Software-Abhängigkeiten?
  - Standard-Funktionen wie bspw. Logging werden in Anwendungen in der Regeln nicht selbst implementiert

Software-Abhängigkeiten & Sicherheitslücken

- Warum Software-Abhängigkeiten?
  - Standard-Funktionen wie bspw. Logging werden in Anwendungen in der Regeln nicht selbst implementiert
- Warum sind Sicherheitslücken hier problematisch?
  - in weit verbreiteten Bibliotheken sind Sicherheitslücken eine „gut dokumentierte“ Möglichkeit eine Anwendung anzugreifen

Software-Abhängigkeiten & Sicherheitslücken

- Für wen ist das problematisch?
  - Ops / Betrieb

Software-Abhängigkeiten & Sicherheitslücken

- Für wen ist das problematisch?
  - Ops / Betrieb
- Wer muss das Problem lösen?
  - Kurzfristig: Ops / Betrieb
  - Langfristig: Dev / Entwicklung

Software-Abhängigkeiten & Sicherheitslücken

- Für wen ist das problematisch?
  - Ops / Betrieb
- Wer muss das Problem lösen?
  - Kurzfristig: Ops / Betrieb
  - Langfristig: Dev / Entwicklung
- => DevSecOps

Was tun?

Betroffen von der Sicherheitslücke ist Log4j von Version 2.0-beta9 bis 2.14.1. Das Apache-Projekt hat kurzfristig Version 2.15.0 veröffentlicht, die die Lücke schließt. In einer Sicherheitsmeldung listen die Apache-Entwickler zudem Maßnahmen auf, wie man die Server ohne Update vorläufig sichern kann. Bei Log4j ab Version 2.10 helfe das Setzen der Systemeigenschaft "`log4j2.formatMsgNoLookups`" auf "`true`" oder das Entfernen der `JndiLookup`-Klasse aus dem Klassenpfad (etwa mit dem Befehl `zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class`).

Quelle: https://www.heise.de/news/Kritische-Zero-Day-Luecke-in-log4j-gefaehrdet-zahlreiche-Server-und-Apps-6291653.html

Was tun?

Die Zero-Day-Lücke Log4Shell hat bereits eine CVE-Nummer erhalten (CVE-2021-44228, Risiko **kritisch, CVSSv3 10/10**). Sie reißt in zahlreiche Dienste und Anwendungen Sicherheitslücken, die die Log4j-Bibliothek einsetzen. Die Pen-Testing-Gruppe 0x0021h schreibt zu ihrem PoC-Exploit, dass er für Apache Struts2, Apache Solr, Apache Druid, Apache Flink und weitere funktioniere.

Quelle: https://www.heise.de/news/Kritische-Zero-Day-Luecke-in-log4j-gefaehrdet-zahlreiche-Server-und-Apps-6291653.html

Quelle: https://www.einfachvorlesen.de/geschichten/der-tag-dem-oma-das-internet-kaputt-gemacht-hat?bonus=toll

CPE, CVE und CWE und CVSS

cpe:/a:apache:poi:3.17

Common Plattform Enumerations (CPE)

CPE Summary

Return to Search Listing

CPE Names

Version 2.3: **cpe:2.3:a:apache:poi:3.17:*:*:*:*:*:*:***

Version 2.2: **cpe:/a:apache:poi:3.17**

Read information about CPE Name encoding

CPE NAME COMPONENTS SELECT A COMPONENT TO SEARCH FOR SIMILAR CPES

Part: a
Vendor: apache
Product: poi
Version: 3.17

QUICK INFO

Created On: 06/18/2019
Last Modified On: 06/18/2019

Metadata

Titles:

Text	Locale
Apache Software Foundation POI 3.17	en_US

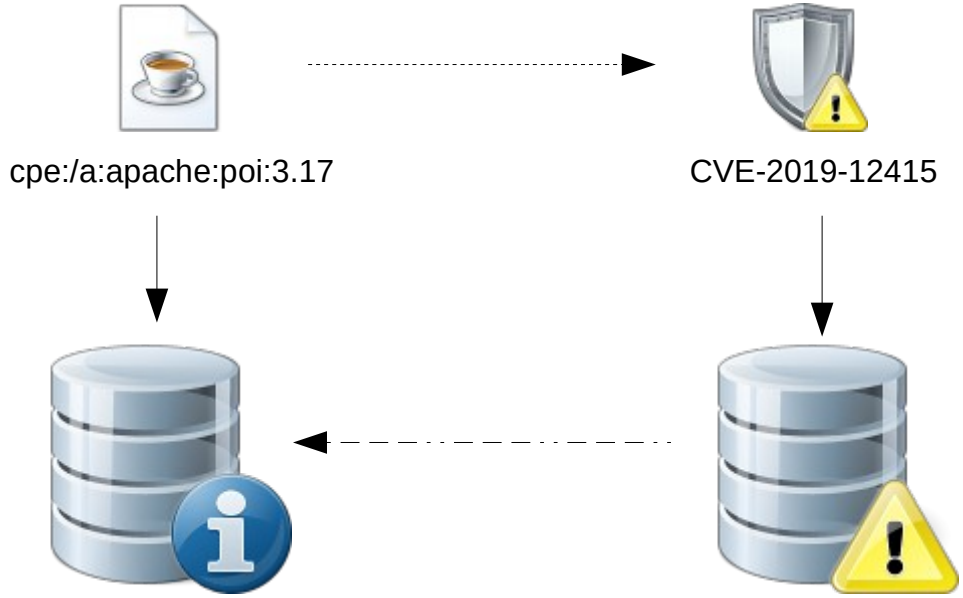
References:

Type	Description	URL
Version	Apache POI Changelog	http://poi.apache.org/changes.html

CPE Usage

View Vulnerabilities

CPE, CVE und CWE und CVSS



Common Plattform Enumerations (CPE) CVE (Common Vulnerabilities and Exposures)

CVE-2019-12415 Detail

Description

In Apache POI up to 4.1.0, when using the tool XSSFExportToXml to convert user-provided Microsoft Excel documents, a specially crafted document can allow an attacker to read files from the local filesystem or from internal network resources via XML External Entity (XXE) Processing.

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 5.5 MEDIUM **Vector:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

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.

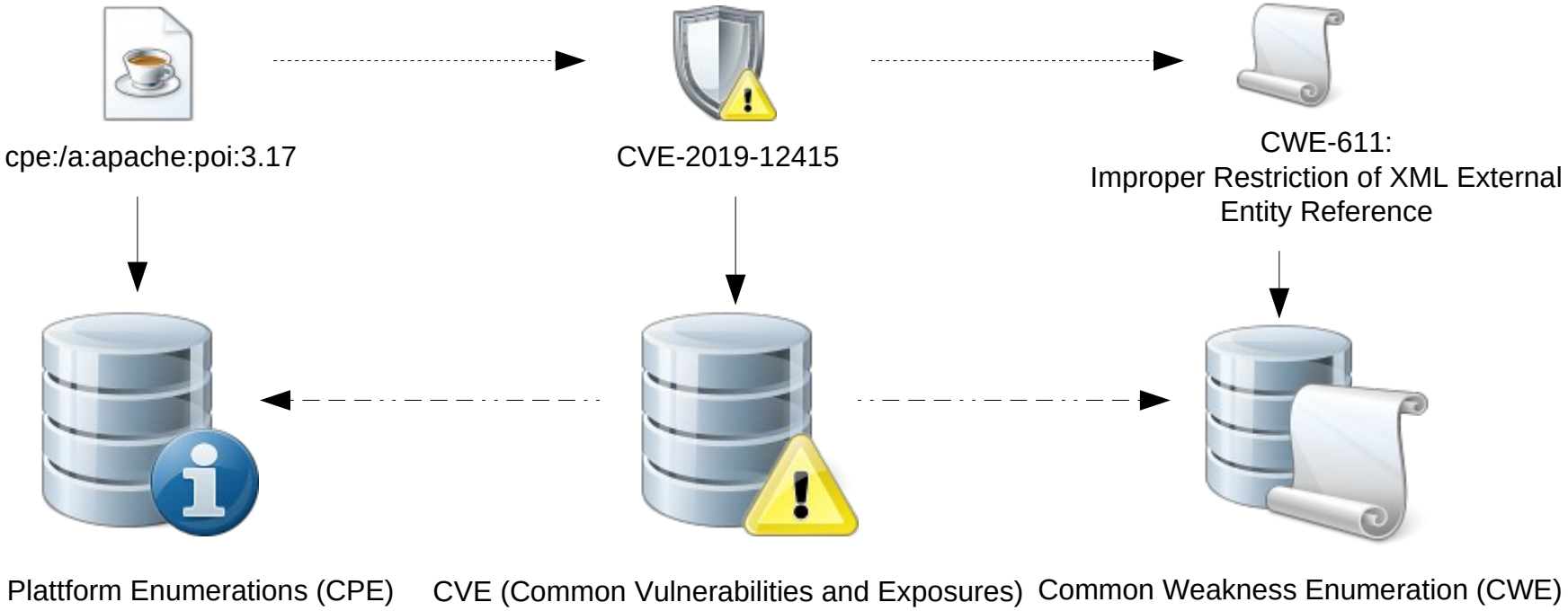
References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

QUICK INFO

CVE Dictionary Entry:
CVE-2019-12415
NVD Published Date:
10/23/2019
NVD Last Modified:
04/08/2022
Source:
Apache Software Foundation

CPE, CVE und CWE und CVSS



CWE-611: Improper Restriction of XML External Entity Reference

Weakness ID: 611
Abstraction: Base
Structure: Simple

View customized information: Conceptual | Operational | Mapping-Friendly | **Complete**

Description

The product processes an XML document that can contain XML entities with URIs that resolve to documents outside of the intended sphere of control, causing the product to embed incorrect documents into its output.

Extended Description

XML documents optionally contain a Document Type Definition (DTD), which, among other features, enables the definition of XML entities. It is possible to define an entity by providing a substitution string in the form of a URI. The XML parser can access the contents of this URI and embed these contents back into the XML document for further processing.

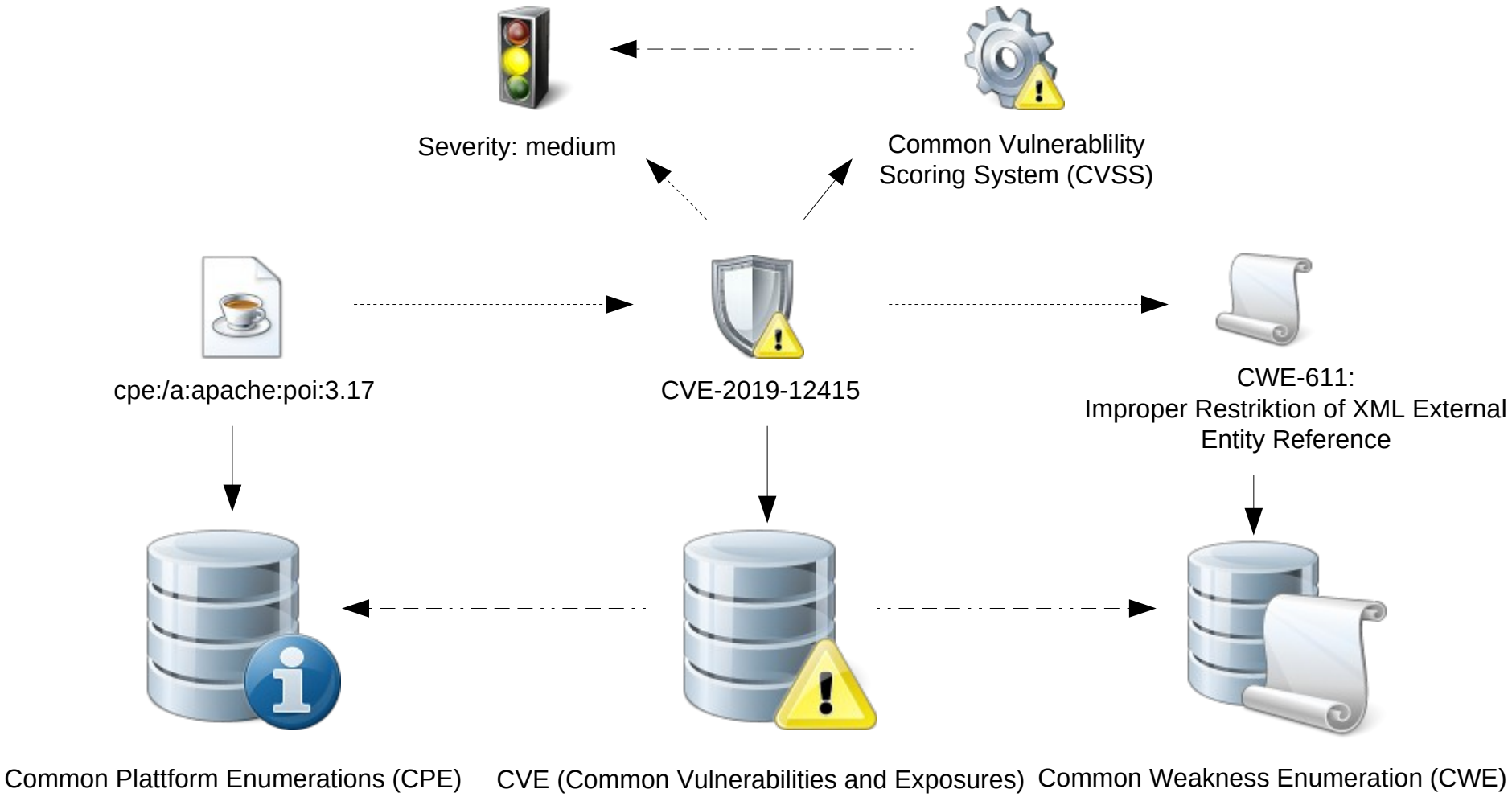
By submitting an XML file that defines an external entity with a file:// URI, an attacker can cause the processing application to read the contents of a local file. For example, a URI such as "file:///c:/winnt/win.ini" designates (in Windows) the file C:\Winnt\win.ini, or file:///etc/passwd designates the password file in Unix-based systems. Using URIs with other schemes such as http://, the attacker can force the application to make outgoing requests to servers that the attacker cannot reach directly, which can be used to bypass firewall restrictions or hide the source of attacks such as port scanning.

Once the content of the URI is read, it is fed back into the application that is processing the XML. This application may echo back the data (e.g. in an error message), thereby exposing the file contents.

Alternate Terms

XXE: An acronym used for the term "XML eXternal Entities"

CPE, CVE und CWE und CVSS



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

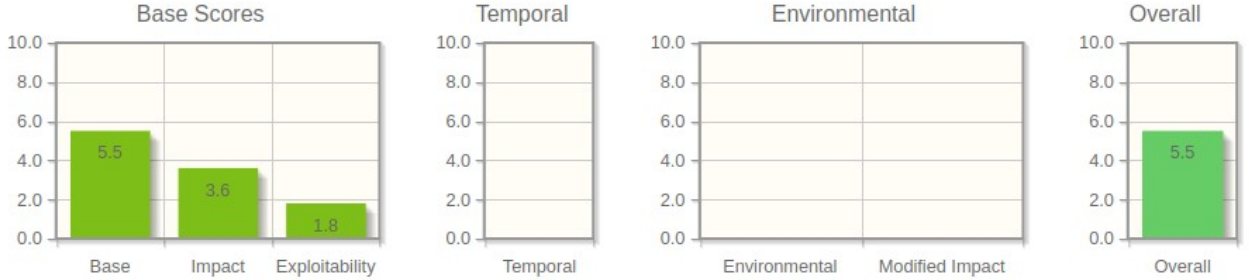
VULNERABILITY METRICS

CVSS Version 3.0 | CVSS Version 3.1

Common Vulnerability Scoring System Calculator CVE-2019-12415

Source: NIST

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequenc such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 5.5
Impact Subscore: 3.6
Exploitability Subscore: 1.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 5.5

Show Equations

CVSS v3.1 Vector

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

Software-Abhängigkeiten?
Abhängigkeiten?
Dependencies?
Bibliotheken?
Frameworks?!

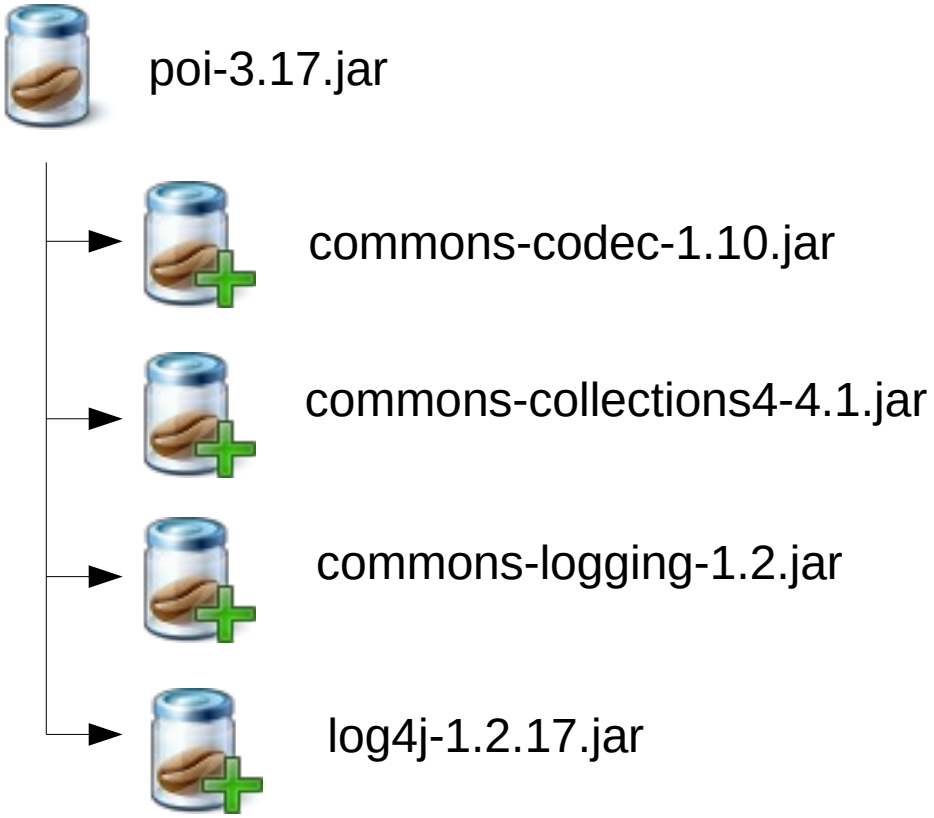
Software-Abhängigkeiten? Abhängigkeiten? Dependencies? Bibliotheken? Frameworks?!

- Bibliotheken oft Teil eines Frameworks mit weiteren abhängigen Bibliotheken

Software-Abhängigkeiten? Abhängigkeiten? Dependencies? Bibliotheken? Frameworks?!

- Bibliotheken oft Teil eines Frameworks mit weiteren abhängigen Bibliotheken
- => transitive Abhängigkeiten

Framework POI 3.17 mit Abhängigkeiten



Quelle: https://www.einfachvorlesen.de/geschichten/der-tag-dem-oma-das-internet-kaputt-gemacht-hat?bonus=toll

Was tun? Wie beurteilen?

- Art der Sicherheitslücke
  - Ausnutzung in Anwendung möglich?
  - Wahrscheinlichkeit?
  - Möglicher Schaden?
  - „subjektiv“

Was tun? Wie beurteilen?

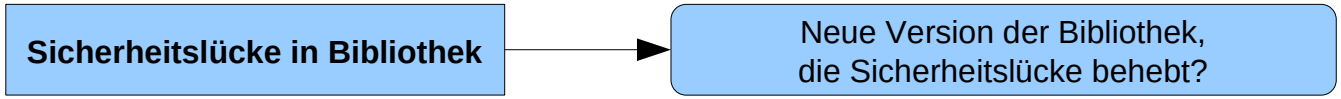
- Art der Sicherheitslücke
  - Ausnutzung in Anwendung möglich?
  - Wahrscheinlichkeit?
  - Möglicher Schaden?
  - „subjektiv“
- Kritikalität gemäß CVSS
  - „objektiv“

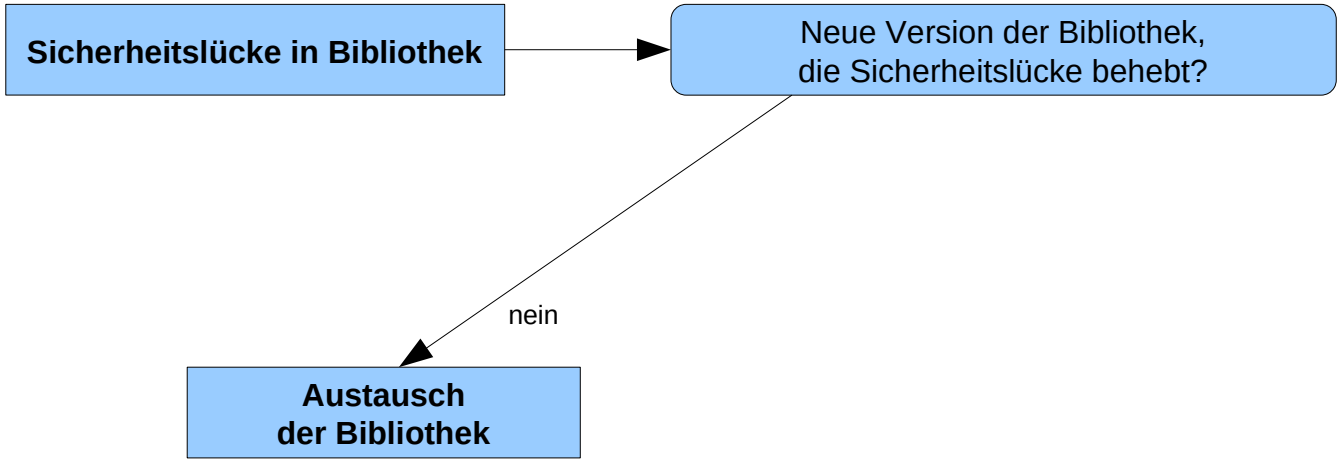
Was tun? Wie beurteilen?

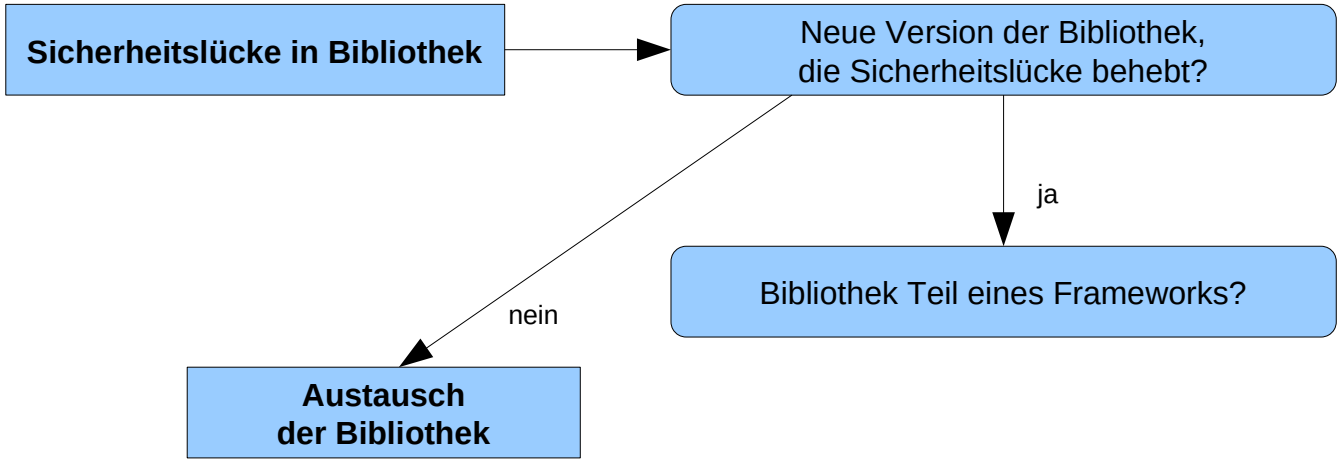
- Beispiel POI 3.17
  - CVE-2019-12415
  - Kritikalität medium
    - In Apache POI up to 4.1.0, when using the tool XSSFExportToXml to convert user-provided Microsoft Excel documents, a specially crafted document can allow an attacker to read files from the local filesystem or from internal network resources via XML External Entity (XXE) Processing

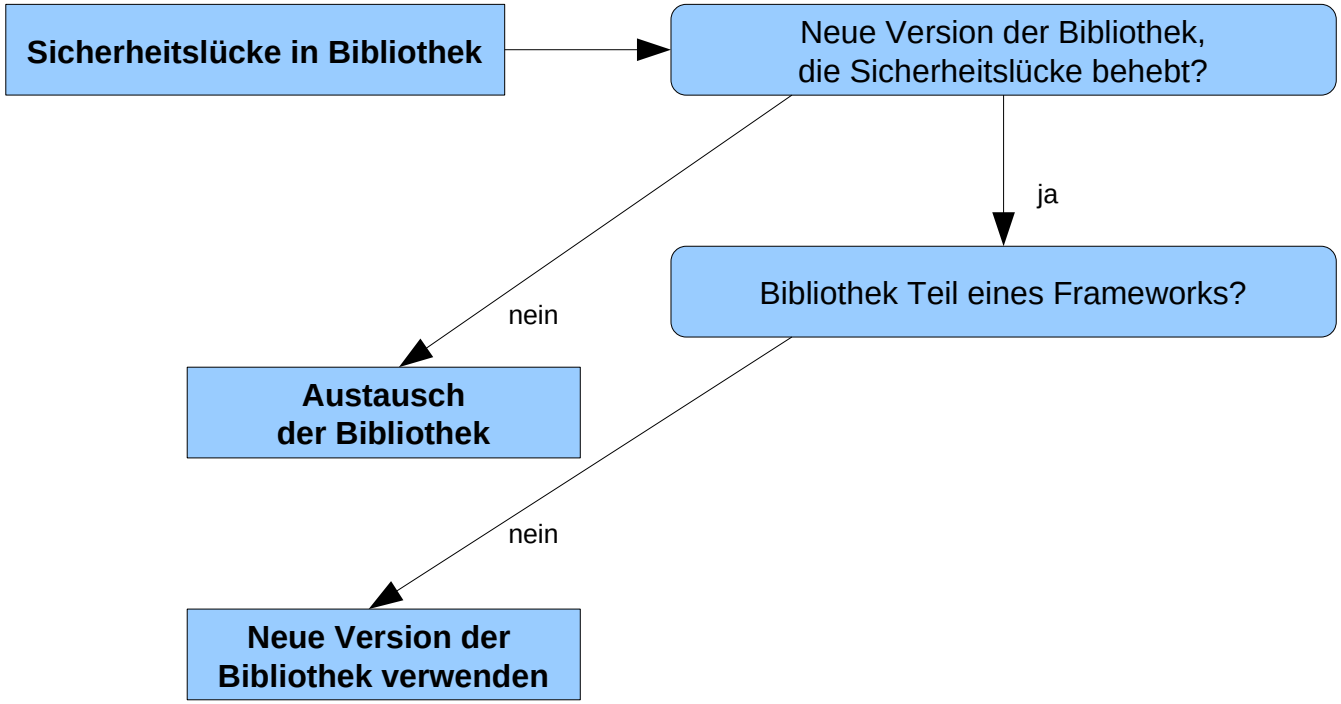
Was tun? Wie beurteilen?

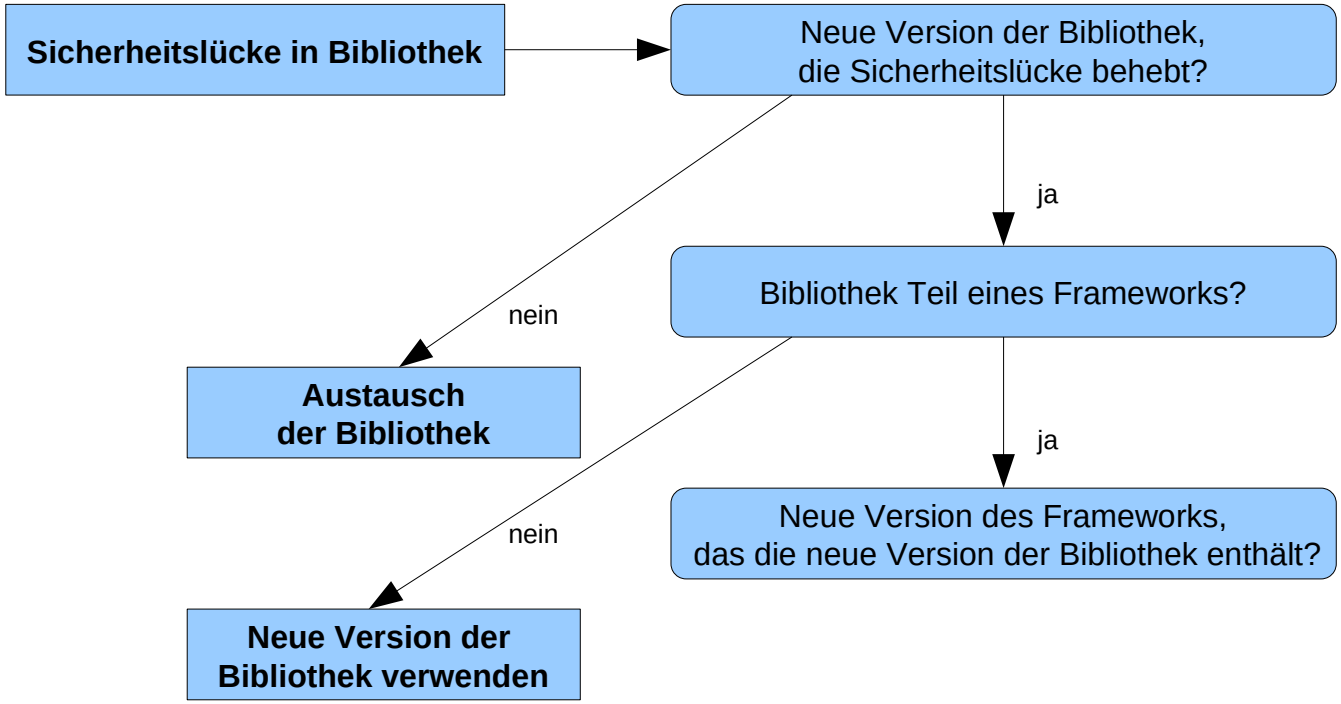
- Beispiel POI 3.17
  - CVE-2019-12415
  - Kritikalität medium
    - In Apache POI up to 4.1.0, when using the tool XSSFExportToXml to convert user-provided Microsoft Excel documents, a specially crafted document can allow an attacker to read files from the local filesystem or from internal network resources via XML External Entity (XXE) Processing
- Entscheidung: Bibliothek mit Sicherheitslücken darf nicht in der Anwendung verbleiben.

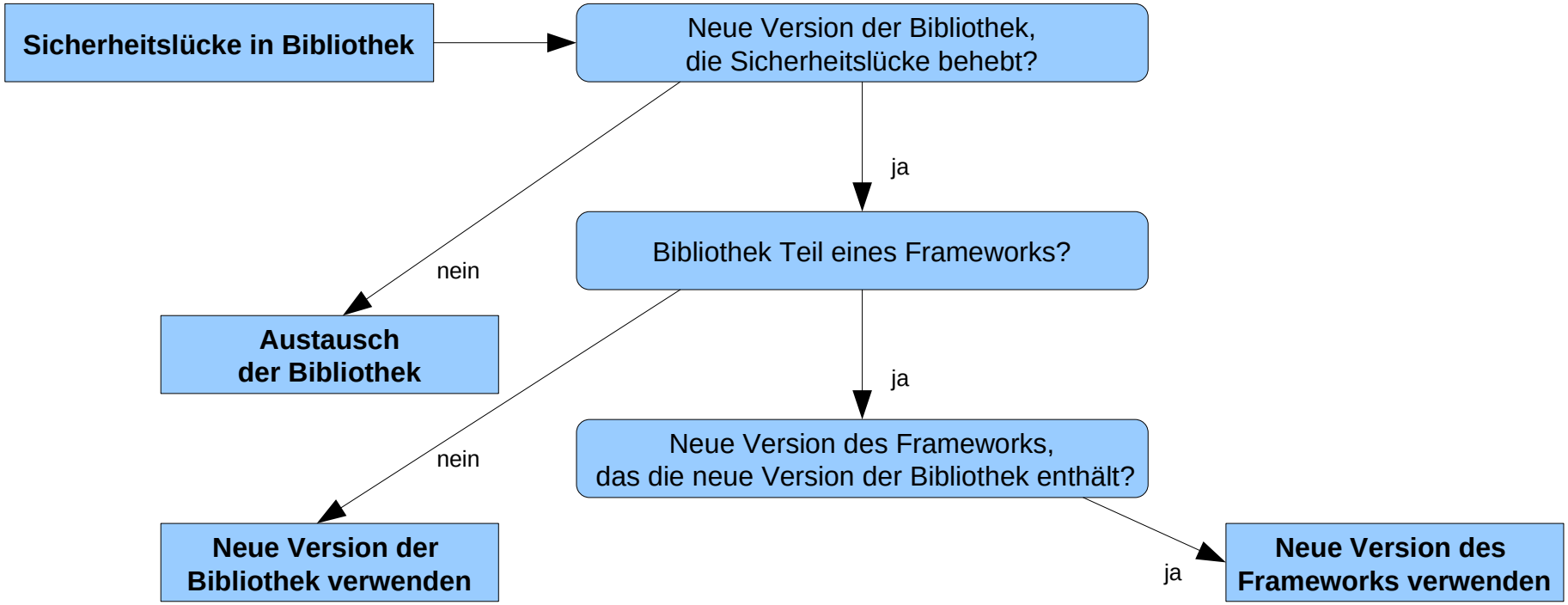

Sicherheitslücke in Bibliothek
Neue Version der Bibliothek,
die Sicherheitslücke behebt?

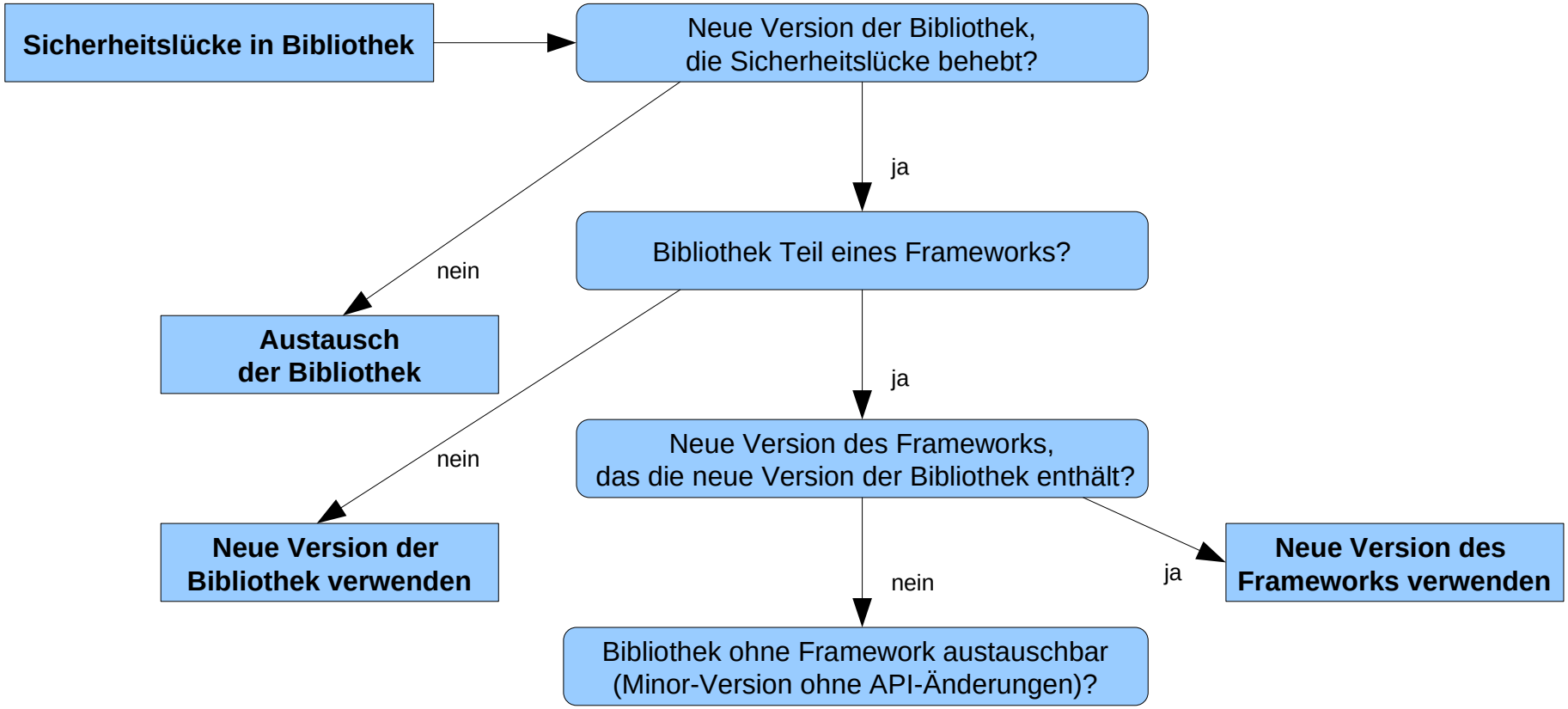

Sicherheitslücke in Bibliothek
Neue Version der Bibliothek,
die Sicherheitslücke behebt?
nein
Austausch
der Bibliothek

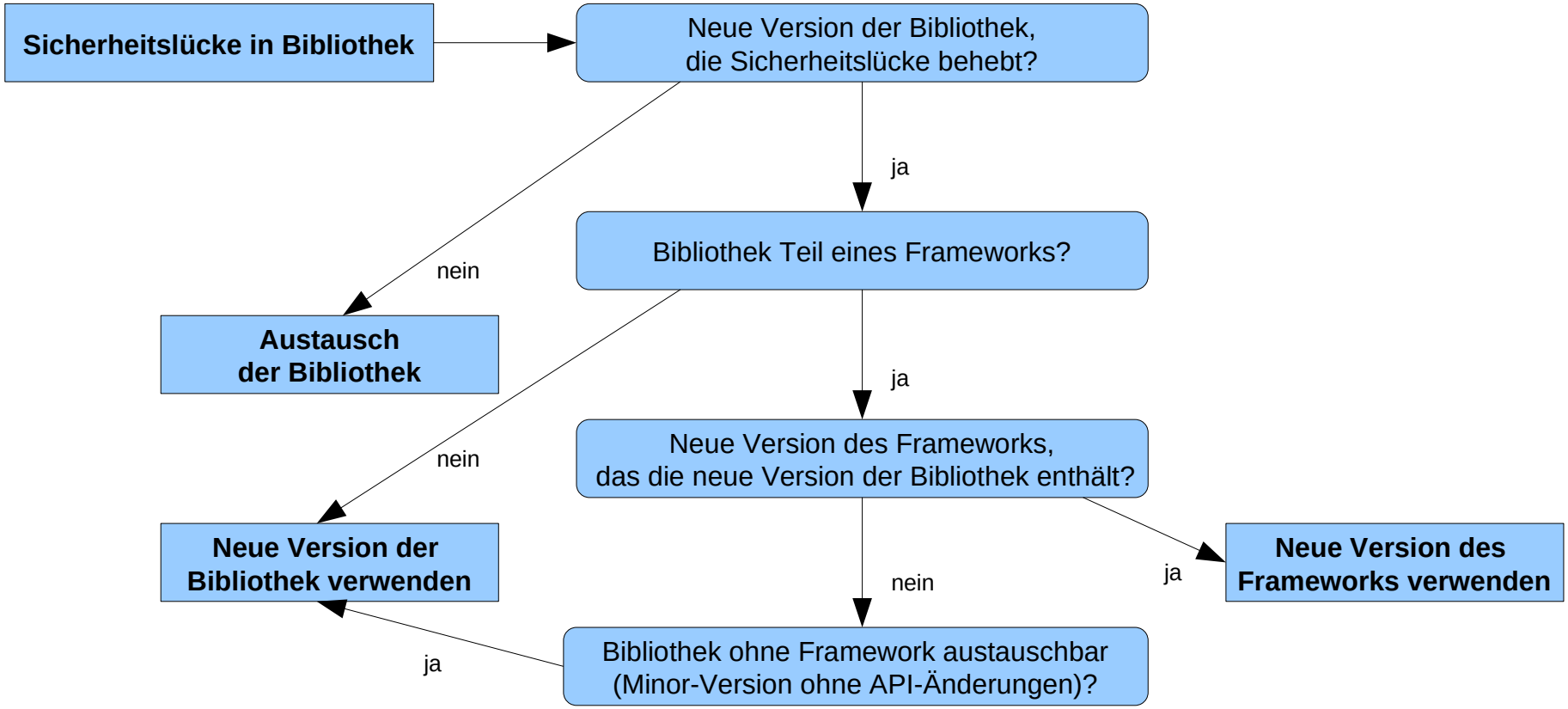

Sicherheitslücke in Bibliothek
Neue Version der Bibliothek, die Sicherheitslücke behebt?
ja
Bibliothek Teil eines Frameworks?
nein
Austausch der Bibliothek

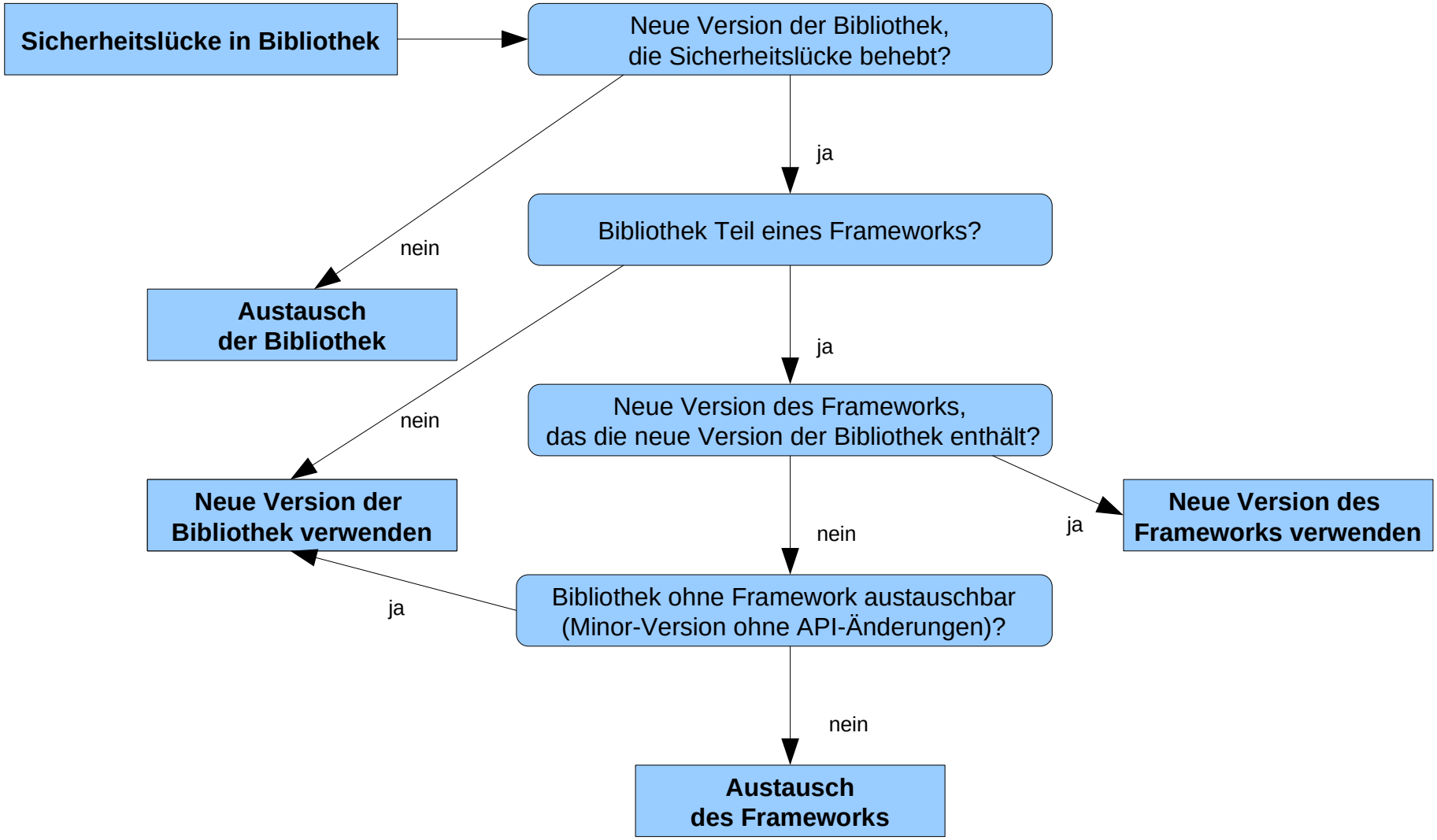

Sicherheitslücke in Bibliothek
Neue Version der Bibliothek, die Sicherheitslücke behebt?
ja
nein
Bibliothek Teil eines Frameworks?
Austausch der Bibliothek
nein
Neue Version der Bibliothek verwenden

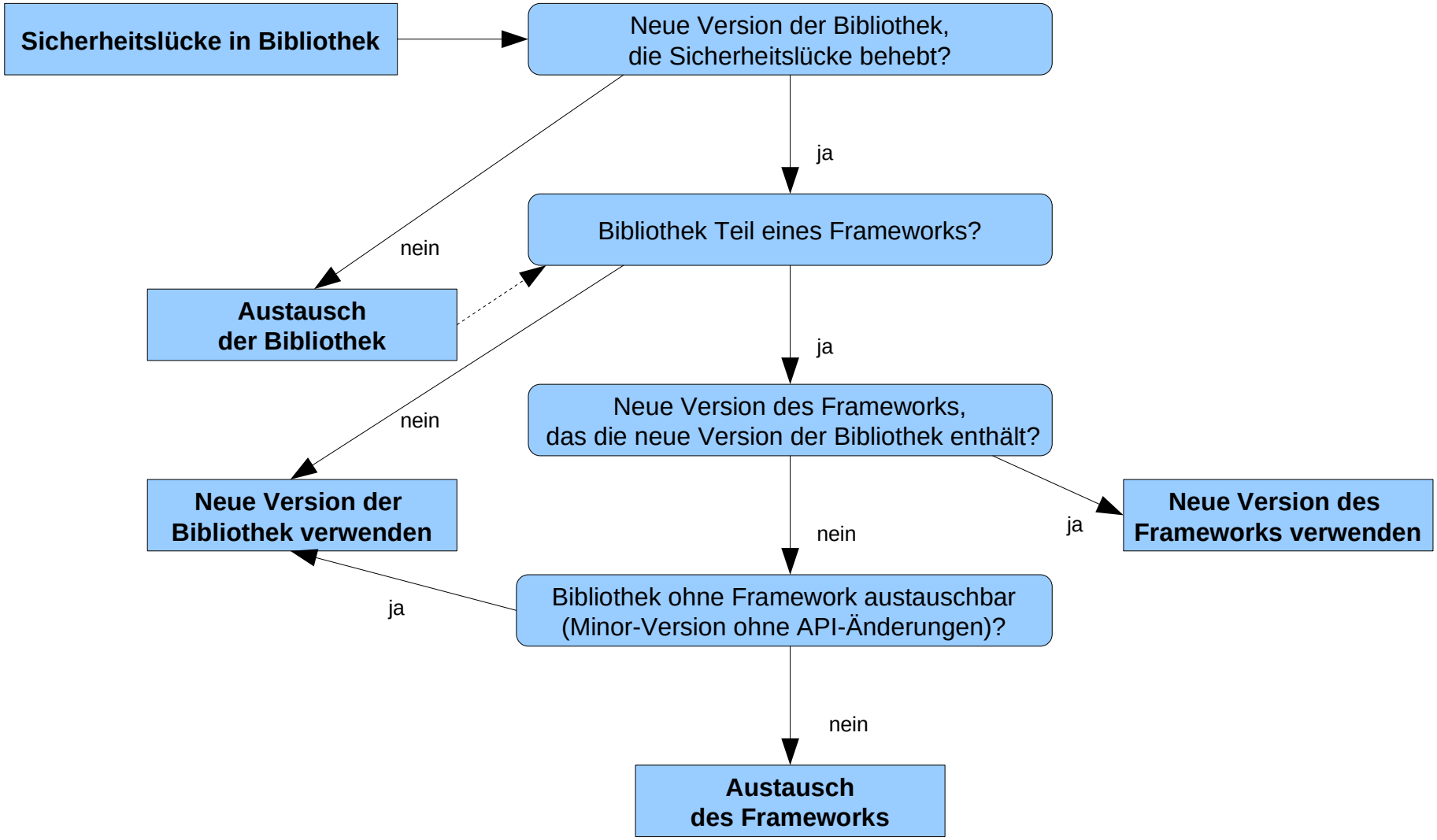

Sicherheitslücke in Bibliothek
Neue Version der Bibliothek, die Sicherheitslücke behebt?
ja
nein
Bibliothek Teil eines Frameworks?
Austausch der Bibliothek
ja
nein
Neue Version des Frameworks, das die neue Version der Bibliothek enthält?
Neue Version der Bibliothek verwenden

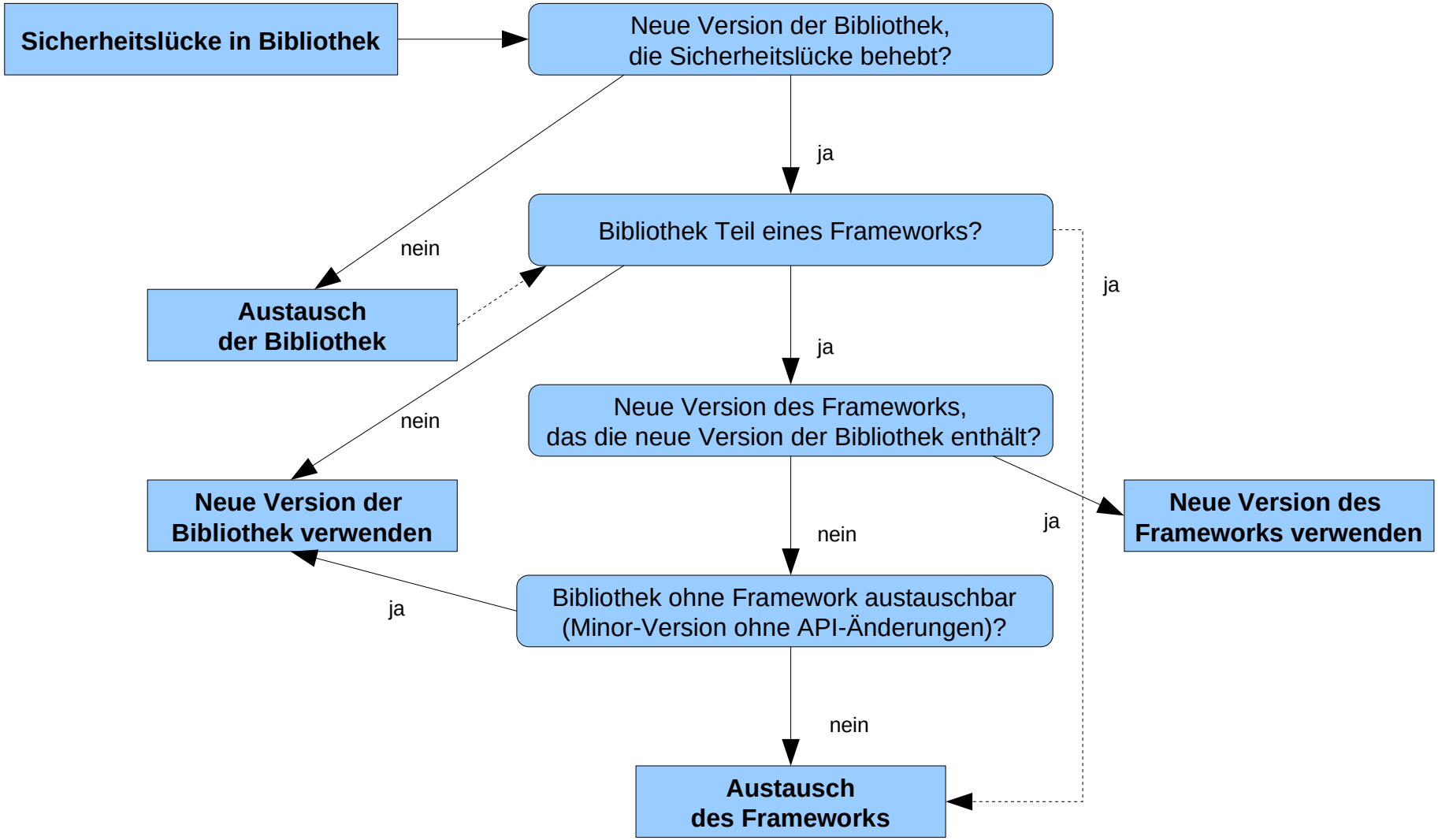

Sicherheitslücke in Bibliothek
Neue Version der Bibliothek, die Sicherheitslücke behebt?
ja
nein
Bibliothek Teil eines Frameworks?
Austausch der Bibliothek
ja
nein
Neue Version des Frameworks, das die neue Version der Bibliothek enthält?
Neue Version der Bibliothek verwenden
ja
Neue Version des Frameworks verwenden


Sicherheitslücke in Bibliothek
Neue Version der Bibliothek, die Sicherheitslücke behebt?
ja
nein
Austausch der Bibliothek
Bibliothek Teil eines Frameworks?
ja
nein
Neue Version der Bibliothek verwenden
Neue Version des Frameworks, das die neue Version der Bibliothek enthält?
ja
Neue Version des Frameworks verwenden
nein
Bibliothek ohne Framework austauschbar (Minor-Version ohne API-Änderungen)?


Sicherheitslücke in Bibliothek
Neue Version der Bibliothek, die Sicherheitslücke behebt?
ja
nein
Austausch der Bibliothek
Bibliothek Teil eines Frameworks?
ja
nein
Neue Version des Frameworks, das die neue Version der Bibliothek enthält?
Neue Version der Bibliothek verwenden
ja
Neue Version des Frameworks verwenden
nein
ja
Bibliothek ohne Framework austauschbar (Minor-Version ohne API-Änderungen)?


Sicherheitslücke in Bibliothek
Neue Version der Bibliothek, die Sicherheitslücke behebt?
ja
nein
Austausch der Bibliothek
Bibliothek Teil eines Frameworks?
ja
nein
Neue Version der Bibliothek verwenden
Neue Version des Frameworks, das die neue Version der Bibliothek enthält?
ja
Neue Version des Frameworks verwenden
nein
ja
Bibliothek ohne Framework austauschbar (Minor-Version ohne API-Änderungen)?
nein
Austausch des Frameworks


Sicherheitslücke in Bibliothek
Neue Version der Bibliothek, die Sicherheitslücke behebt?
ja
nein
Bibliothek Teil eines Frameworks?
Austausch der Bibliothek
ja
nein
Neue Version des Frameworks, das die neue Version der Bibliothek enthält?
Neue Version der Bibliothek verwenden
ja
Neue Version des Frameworks verwenden
nein
ja
Bibliothek ohne Framework austauschbar (Minor-Version ohne API-Änderungen)?
nein
Austausch des Frameworks


Sicherheitslücke in Bibliothek
Neue Version der Bibliothek, die Sicherheitslücke behebt?
ja
nein
Bibliothek Teil eines Frameworks?
ja
Austausch der Bibliothek
ja
nein
Neue Version des Frameworks, das die neue Version der Bibliothek enthält?
Neue Version der Bibliothek verwenden
ja
Neue Version des Frameworks verwenden
nein
ja
Bibliothek ohne Framework austauschbar (Minor-Version ohne API-Änderungen)?
nein
Austausch des Frameworks

Quelle: https://www.einfachvorlesen.de/geschichten/der-tag-dem-oma-das-internet-kaputt-gemacht-hat?bonus=toll

OWASP Dependency Check & Jenkins Plugin

- OWASP Dependency Check
  - Open Worldwide Application Security Project
  - Dependency Check: Tool

OWASP Dependency Check & Jenkins Plugin

- OWASP Dependency Check
  - Open Worldwide Application Security Project
  - Dependency Check: Tool
  - Finden von <u>öffentlich bekannten</u> Sicherheitslücken in Abhängigkeiten
    - findet CPE zur Abhängigkeit
    - erzeugt Report, der Abhängigkeit, CPE und zugehörige CVE verknüpft

OWASP Dependency Check & Jenkins Plugin

- OWASP Dependency Check
  - Open Worldwide Application Security Project
  - Dependency Check: Tool
  - Finden von <u>öffentlich bekannten</u> Sicherheitslücken in Abhängigkeiten
    - findet CPE zur Abhängigkeit
    - erzeugt Report, der Abhängigkeit, CPE und zugehörige CVE verknüpft
- Jenkins Plugin
  - https://plugins.jenkins.io/dependency-check-jenkins-plugin/
  - Alternativ z.B. Maven, Gradle, …

OWASP Dependency Check & Jenkins Plugin

- Projekt-Beispiel
  - CI Jenkins bereits vorhanden
  - wöchentlicher Job
  - eigener Job nur für Prüfung von Sicherheitslücken

Jenkins-Plugin: Aufruf Build

Invoke Dependency-Check

Dependency-Check installation

Dependency-Check 5.1.1

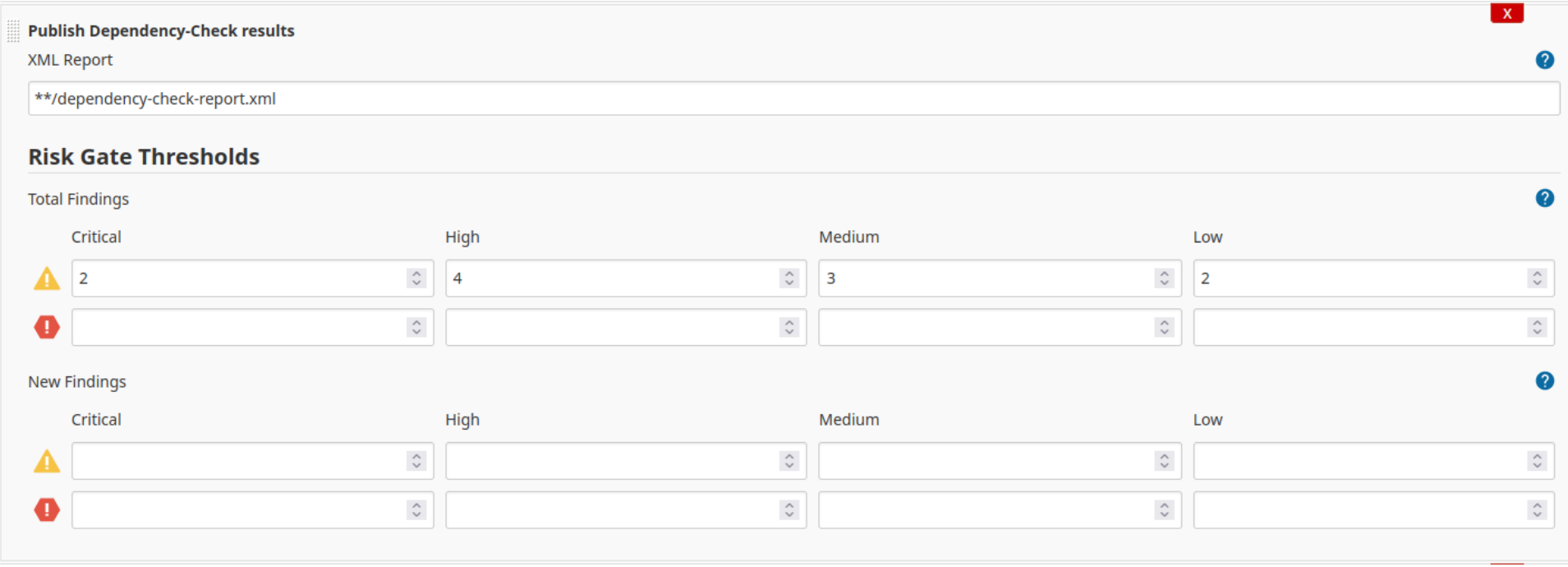
Arguments

```
--exclude **/[illegible]/libs/test/junit.jar
--exclude **/[illegible]/libs/compiling/jackson-databind.jar
--exclude **/[illegible]/libs/test/junit.jar
--exclude **/[illegible]/end2end/loginutils.jar
```

☐ Skip if triggered by SCM changes

☐ Skip if triggered by upstream changes

Jenkins-Plugin: Aufruf Post-Build



Jenkins-Plugin: Ergebnisse 1/3

Dependency-Check Results

SEVERITY DISTRIBUTION

1	3	2	1

Search

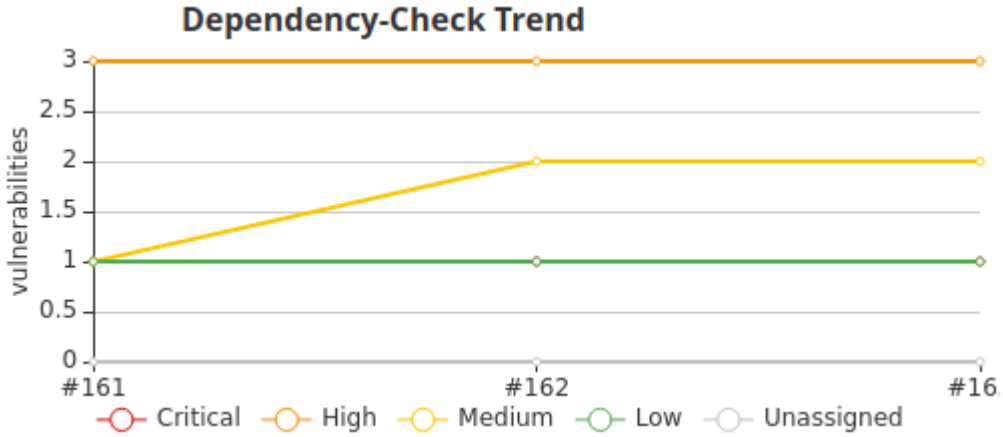
File Name	Vulnerability	Severity	Weakness
poi-3.17.jar	NVD CVE-2019-12415	Medium	CWE-611
log4j-1.2.17.jar	NVD CVE-2019-17571	Critical	CWE-502
log4j-1.2.17.jar	NVD CVE-2020-9488	Low	CWE-295
log4j-1.2.17.jar	OSSINDEX CVE-2021-4104	High	
xmlgraphics-commons-2.3.jar	OSSINDEX CVE-2020-11988	Medium	
batik-all-1.10.jar	NVD CVE-2019-17566	High	CWE-20
batik-all-1.10.jar	NVD CVE-2020-11987	High	CWE-20

Jenkins-Plugin: Ergebnisse 2/3

poi-3.17.jar | NVD CVE-2019-12415 | Medium | CWE-611

File Path	/var/lib/jenkins/workspace/[illegible]/WebContent/WEB-INF/lib/poi-3.17.jar
SHA-1	0ae92292a2043888b40d418da97dc0b669fde326
SHA-256	30181821dd2e849727b638b9e329aeff4a64f3445c4142b13cf7a18bb3552edd
Description	In Apache POI up to 4.1.0, when using the tool XSSFExportToXml to convert user-provided Microsoft Excel documents, a specially crafted document can allow an attacker to read files from the local filesystem or from internal network resources via XML External Entity (XXE) Processing.

Jenkins-Plugin: Ergebnisse 3/3



Quelle: https://www.einfachvorlesen.de/geschichten/der-tag-dem-oma-das-internet-kaputt-gemacht-hat?bonus=toll

Vorgehen & Maßnahmen

- Unstable → E-Mail an „Sicherheits-Experten“
  - Sicherheits-Experte = Rolle
  - Einzelner Entwickler, Architekt oder Entwickler-Team

Vorgehen & Maßnahmen

- Unstable → E-Mail an „Sicherheits-Experten“
  - Sicherheits-Experte = Rolle
  - Einzelner Entwickler, Architekt oder Entwickler-Team
- 2do: Ursache prüfen und beurteilen!

Vorgehen & Maßnahmen

- Unstable → E-Mail an „Sicherheits-Experten“
  - Sicherheits-Experte = Rolle
  - Einzelner Entwickler, Architekt oder Entwickler-Team
- 2do: Ursache prüfen und beurteilen!
- Mögliche Maßnahmen
  - Bibliothek als exclude hinzufügen
  - Grenzwerte anpassen („known vulnerabilities“)
  - Ersetzung der Bibliothek einplanen
    - Bsp. POI 3.17 auf min. POI 4.1.0 anheben

Quelle: https://www.einfachvorlesen.de/geschichten/der-tag-dem-oma-das-internet-kaputt-gemacht-hat?bonus=toll

Grenzen & Fazit

- Grenzen
  - Sicherheitslücken im Anwendungscode
  - Custom Bibliotheken

Grenzen & Fazit

- Grenzen
  - Sicherheitslücken im Anwendungscode
  - Custom Bibliotheken
- Fazit
  - kein „silver bullet“
  - frühzeitig Hinweise auf Sicherheitslücken
  - man hat die Möglichkeit zu reagieren

Quelle: https://www.einfachvorlesen.de/geschichten/der-tag-dem-oma-das-internet-kaputt-gemacht-hat?bonus=toll