Log4Shell ふりかえり

JANOG49 ライトニングトーク

谷岡 英治
シスコシステムズ合同会社
2022年1月26日

前置き

本発表及び資料は発表者が個人で調査、検証、考察したものであり、
所属組織の公式見解ではありません。

某所にて

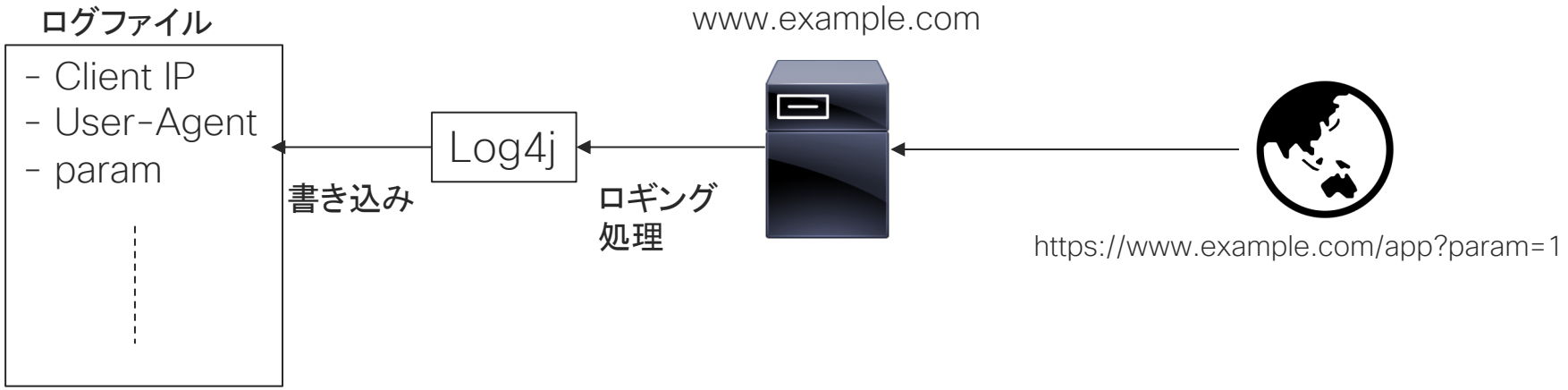
- なんかヤバいセキュリティ問題が出てるらしい。
- Log4j関連らしいよ。
  - なんでロギング用のライブラリで…？

調査してみた

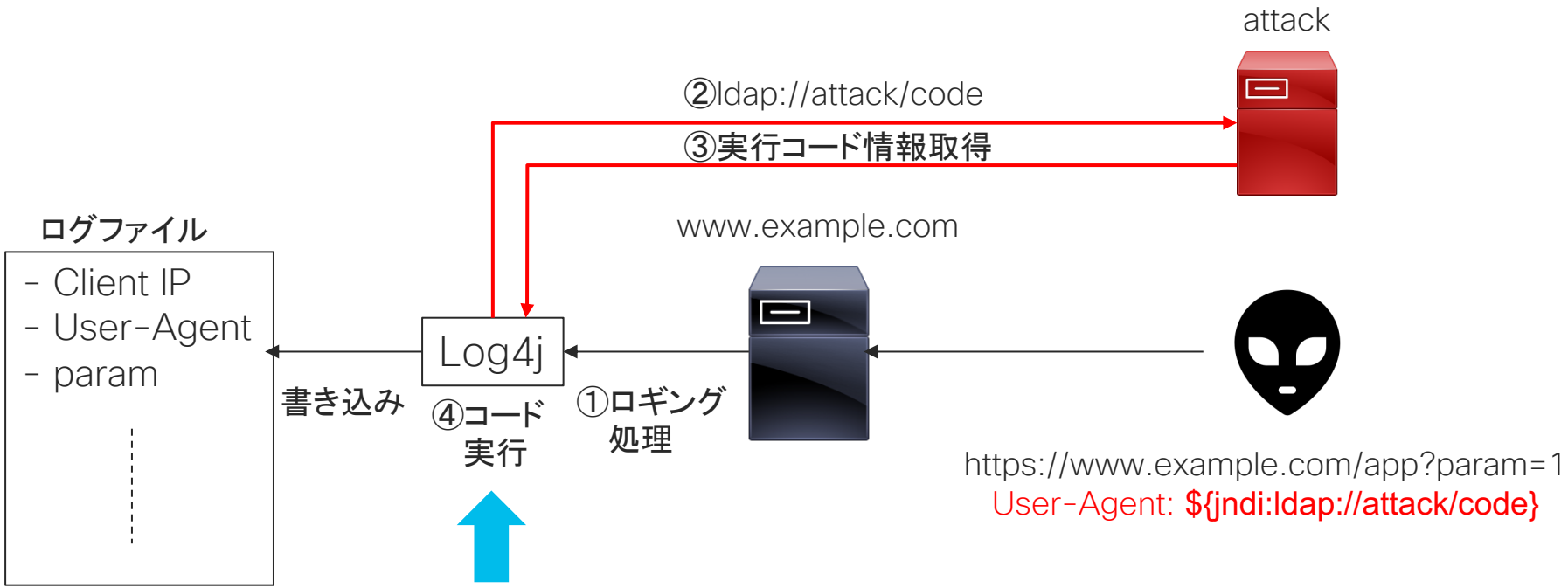
詳細は
https://logging.apache.org/log4j/2.x/security.html

- CVE-2021-44228: 外部から渡された文字列に含まれる URL や内部パスに設置されたコードを JNDI Lookup 機能を介して実行可能。（CVSSスコア: 10.0）
- その後さらに…
  - CVE-2021-45046: CVE-2021-44228の修正が不十分なため、特定の設定がデフォルトから変更されている場合に情報漏洩、リモートコード実行、ローカルコード実行が可能。（CVSSスコア:9.0）
  - CVE-2021-45105: 特定の設定がデフォルトから変更されている場合に、再帰処理の無限ループによるDoS攻撃が実行可能。（CVSSスコア:5.9）
  - CVE-2021-44832: 攻撃者がロギング設定ファイルを変更できる場合に、JDBC Appenderを使ったリモートコード実行が可能。（CVSSスコア:6.6）

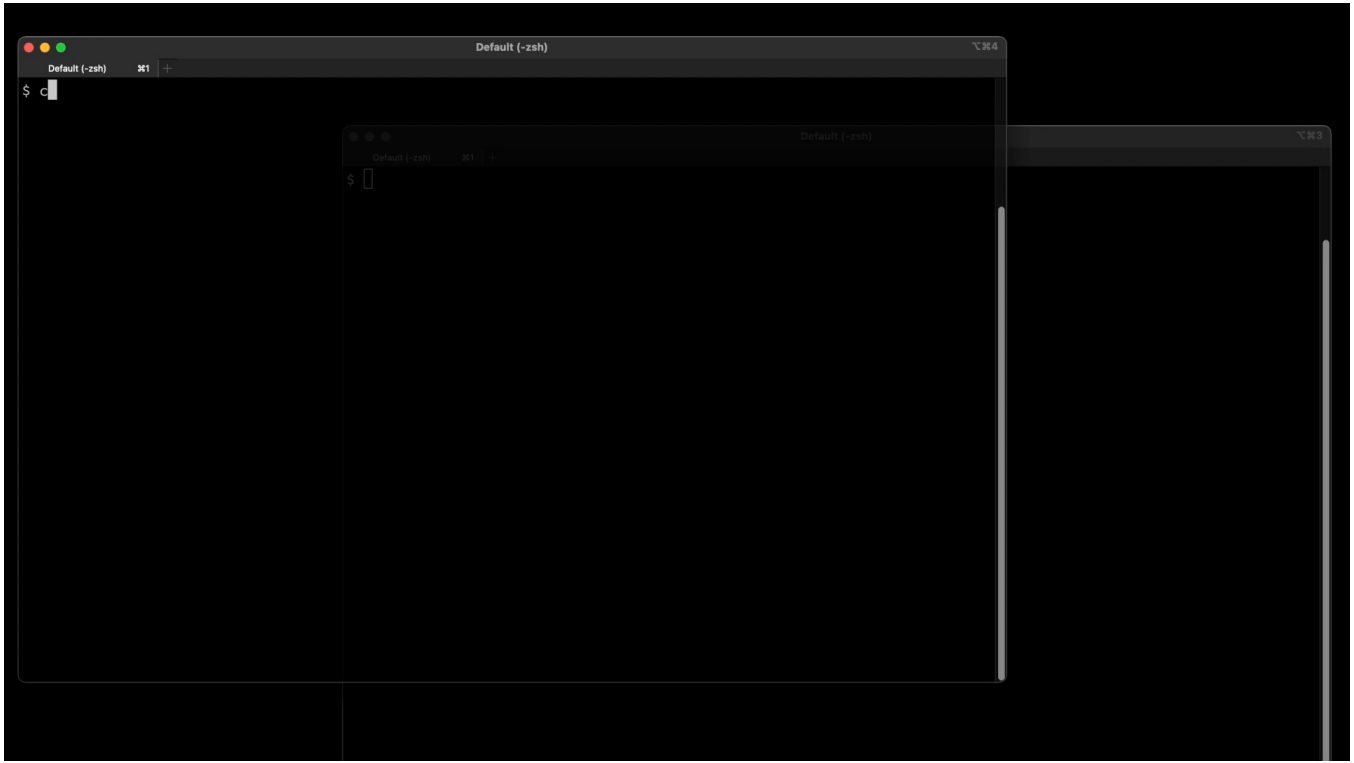
通常のLog4jの使われ方



RCE実行パターン



検証してみた



JNDIって何？

- Java Naming and Directory Interface
  - 名前とJavaオブジェクトを結びつけるためのAPI
  - DNS, LDAPなどのサービスに登録された情報から、実行する内容を取得する
  - データベース接続情報（接続先、データベースタイプ、クレデンシャル等）のようなものをLookup（検索）して使用することで、コードにこれらの情報を記述しないで済むようになる

JNDI自体は特別な機能ではない

なぜ影響が大きかったのか

- 外部からの実行が容易
  - 文字列を生成して送りつけるだけ
  - ログに書き込まれそうなところならどこでも使える
  - LDAP/DNSによる外向きアクセス→フィルタされていない
  - 勝手に実行される
- 有効になっている環境が多い
  - デフォルトで有効（設定ファイルで意図的に無効にしていない限り有効）

対策

色々とワークアラウンドは出ましたが、結局は

バージョンアップ

現在：2.17.1

※Log4j 1.x系はEOLなので、

既知の問題も修正されません。

Ciscoの対応状況

- Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021
  - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd
- **シスコ製品に影響を与える** Apache Log4j **ライブラリの脆弱性**：2021 **年** 12 **月**
  - https://www.cisco.com/c/ja_jp/support/docs/csa/2021/cisco-sa-apache-log4j-qRuKNEbd.html
- Threat Advisory: Critical Apache Log4j vulnerability being exploited in the wild
  - https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html

事前にできたことはあったのか

- 開発者（ライブラリ利用者として）
  - 設定項目の精査
    - 使用しない機能は「明示的に」無効化する。
      →IOSの「no ip domain lookup」や「no ip http server」のようなこと
    - デフォルト設定をそのまま使うのではなく、実環境に合わせた設定にする。
      →IOSの「transport input ssh」のようなこと
  - メンテナンスされているバージョンへの追従、EOLやセキュリティfix情報のキャッチアップ
- 運用者（ソフトウェア、サービスの利用者として）
  - アップグレードのルーティン化
    - 「動いているからそのまま」ではなく、いつでもバージョンアップできるように準備。
  - トラフィックのチェック

これからできることはあるのか

- 情報収集
  - Twitter、Slackなど社外コミュニティが発する情報へのアクセス
  - RSSフィードの購読
  - CVE Trends https://cvetrends.com/

- 利用するプロダクトへの関心
  - GIGAZINE:全世界を揺るがした「Log4j」のようなオープンソースソフトウェアを無償でメンテし続けるという難題を解決すべくGoogleが立ちあがる
  - GIGAZINE: 「無料でLog4j対策を教えろ」と迫った大企業とオープンソース開発者の痛快なやりとりが公開中
  - 誰かの成果を無償で使えればそれでいいのか？

The bridge to possible