Apache Log4j に関する解説 1.6版
(2022/2/15)

NTTデータ先端技術株式会社(IL-CSIRT)

【目次】

NTT DATA

Apache Log4j に関する解説

1. 概要

2021/12/5(日本時間)にApache Software Foundationから、Apache Log4j(以下、Log4j)に、任意のコード実行の脆弱性があるという情報が公開※1されました。

なお、2021/12/7(日本時間)に修正版の提供が開始※2※3されています。

2. Log4jとは

- The Apache Software Foundation Projectで開発されているJavaベースのロギング用ライブラリです。
- Log4jを利用することで、デバッグ情報やエラー情報などをプログラム内からログファイル等に出力することができます。
- Log4jはJava等のアプリケーションでログ出力を行なうための実装として広く利用されています。

※1.参考：Limit the protocols JNDI can use and restrict LDAP.
https://issues.apache.org/jira/browse/LOG4J2-3201
※2.参考：Release History
https://logging.apache.org/log4j/2.x/changes-report.html
※3.詳細は「7. 対策方法」を参照

Apache Log4j に関する解説

3. Log4jの脆弱性とは

- 本脆弱性は通称「Log4Shell」と呼ばれ、CVE番号として「CVE-2021-44228」※1が採番されています。
- Log4jに含まれるJNDI Lookup機能※2の問題に起因して、攻撃者にリモートから任意のコードを実行される可能性があります。
- 2021/12/10(日本時間)時点で、本脆弱性を悪用する実証コードが公開※3され、国内にて本脆弱性の悪用を試みる通信が確認されています。

  ⇒報告されている実害例：

  - ランサムウェアなどのマルウェアに感染させられる※4
  - 暗号資産のマイナーを設置される※5

※1.CVE：https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228
※2.JNDI Lookup機能(Java Name and Directory Interface Lookup機能)とは：
Java アプリケーションが DNS や LDAP 等のサービスを利用するための汎用的なライブラリで、出力される情報に特定の文字列が含まれる場合、変数として置換する機能です。この機能を活用することで日付や環境情報などを動的に出力することができます。
※3.参考：Apache Log4j 远程代码执行 (2021.12.20現在、リンク先閉鎖)
https://github.com/tangxiaofeng7/CVE-2021-44228-Apache-Log4j-Rce
※4.参考：2021/12/13 15:02の@80vulによるツイート
https://twitter.com/80vul/status/1470272820571963392
※5.参考：2021/12/11 00:04の@GossiTheDogによるツイート
https://twitter.com/GossiTheDog/status/1469322120840708100

Apache Log4j に関する解説

4. 攻撃の流れ(LDAPを利用した場合の例)

本脆弱性を悪用した攻撃の流れは以下のとおりです。

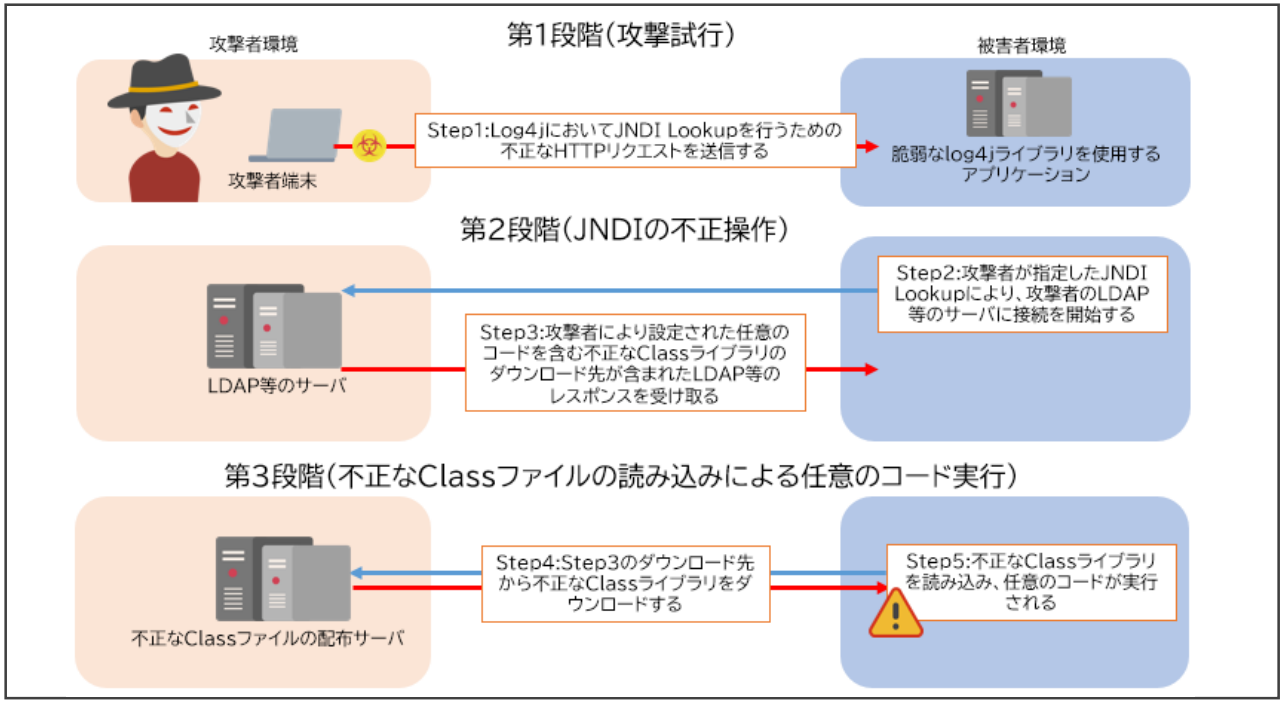
Step1. 攻撃者が、細工した文字列を被害者のサーバに送信し、Log4jは送信されてきた情報をログとして記録する

Step2. 被害者のサーバが、Log4jのJNDI Lookup機能により、Step1で指定された攻撃者のLDAPサーバに接続する

Step3. 攻撃者が、不正なClassライブラリのダウンロード先を記したLDAPのレスポンスを被害者のサーバに返す

Step4. 被害者のサーバが、不正なClassライブラリをダウンロードする

Step5. 被害者のサーバが、不正なClassライブラリに記された任意のコードを読み込み、実行する



Apache Log4j に関する解説

4. 攻撃の流れ(LDAPを利用しない場合の例)

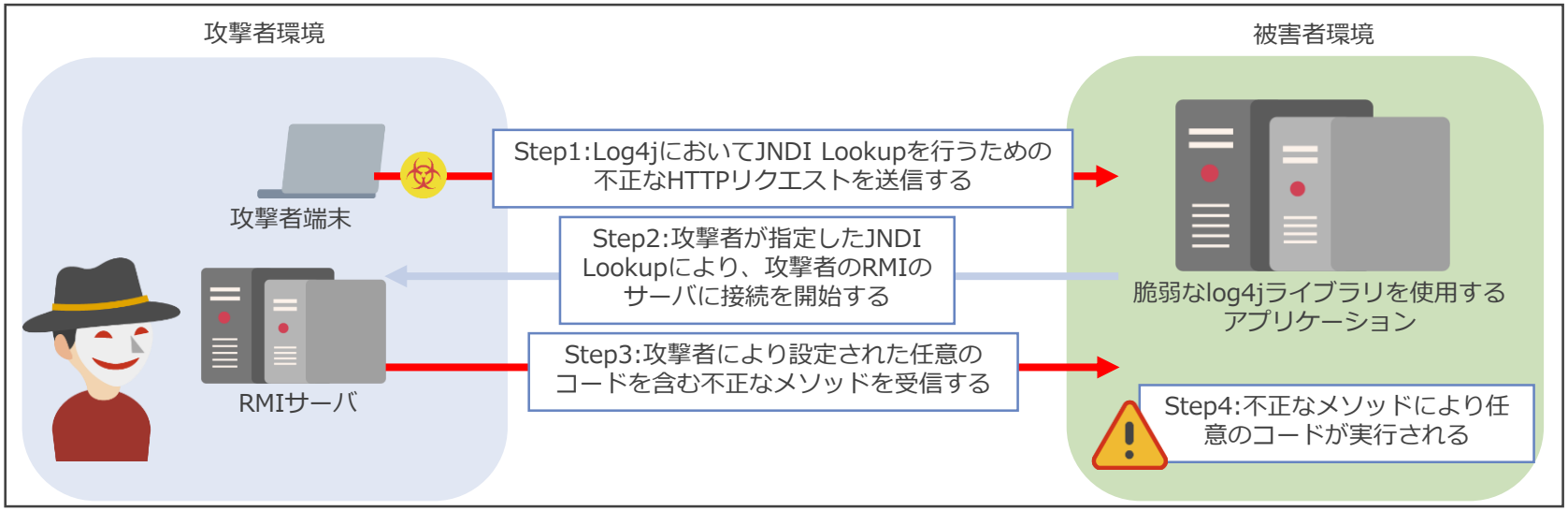
本脆弱性を悪用した攻撃の流れは以下のとおりです。

Step1. 攻撃者が、細工した文字列を被害者のサーバに送信し、Log4jは送信されてきた情報をログとして記録する

Step2. 被害者のサーバが、Log4jのJNDI Lookup機能により、攻撃者のRMIのサーバにリクエストを送信する

Step3. 被害者のサーバが、攻撃者のサーバから攻撃者が用意した任意のコードを含む不正なメソッドをレスポンスとして受信する

Step4. 被害者のサーバが、不正なメソッドに記された任意のコードを読み込み、実行する



Apache Log4j に関する解説

5. 影響対象

Apache Log4j 2.15.0より前の2系のバージョン

※1.End of Lifeを迎えているApache Log4j 1系のバージョンは、遠隔からのコードを実行することはできません。悪意ある第三者が脆弱性を悪用する場合は何らかの方法で事前にシステムに侵入できている必要があります。

※2.個別にインストールされている他、以下のような場合でご利用されている製品やサービスで影響を受けるLog4jが使用されている可能性があります。詳細は製品/サービスベンダにお問い合わせください。
- アプライアンスに含まれる場合
- S/Wパッケージに含まれる場合
- 組み込み機器(IoT等)に含まれる場合

※3.参考：影響を受けるプロダクトについては、オランダ国立サイバーセキュリティセンターがgithub上で情報をとりまとめて公開しています。参照される場合は、随時加筆修正が行われていることを留意の上でご活用ください。
https://github.com/NCSC-NL/log4shell/tree/main/software

Apache Log4j に関する解説

6. 影響有無の確認方法
   現在調査中

Apache Log4j に関する解説

7. 対策方法

The Apache Software Foundationから本脆弱性を修正したバージョンが公開されているため、修正したバージョンに更改してください。

・Apache Log4j 2.16.0以降※1※2※3

※1.2021/12/7(日本時間)に修正バージョンとして公開されたApache Log4j 2.15.0には、2021/12/17(日本時間)に新たに別のリモートコード実行の脆弱性が確認されました。また、当初示されていたLookup機能を無効化するという回避策も対策として不十分であることが確認されました。そのため、Apache Log4j 2.15.0に更改したシステムや回避策を行ったシステムにおいても、当欄記載のバージョンに更改してください。
新たに確認されたリモートコード実行の脆弱性：CVE-2021-45046
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046

※2.2021/12/19(日本時間)に、Apache Log4j 2.16.0に別の脆弱性(Denial of Service)が発見され新しい修正バージョン(Apache Log4j 2.17.0)が公開されるなど、連日大きな動きを見せています。The Apache Software Foundationのサイトなどを随時確認し、自社にとって影響のある脆弱性が確認された場合は、適宜アップデートをするなどの対応を検討してください。

※3.Apache Log4j 2.13.0以降は、動作環境としてJava 8が指定されているため、Java 7以前の環境を使用されている場合は併せて更新が必要となります。なお、2021/12/28(協定世界時)にJava 6とJava 7環境用の修正バージョンが公開されました。Java 6とJava 7は公式サポートが終了しているため、Java 8にアップデートすることが望ましいですが、Java 8への早急なアップデートを行うことが困難な場合は暫定対処として検討してください。
The Apache Software Foundation：https://logging.apache.org/log4j/2.x/

Log4jのバージョン	動作環境
~2.3.x	Java 6以降
2.4 ~ 2.12.x	Java 7以降
2.13.0~	Java 8以降

Apache Log4j に関する解説

8. 当社SOCサービス/製品での検知可否

(2022.2.9現在)

種別	製品ベンダー	製品	製品ベンダー提供のシグネチャ	検知結果
IDS/IPS	IBM	・QRader ・Network Security ・GX/XGS Series	HTTP_Log4J_Form_Lookup_Exec HTTP_Log4J_JndiLdap_Exec HTTP_Log4J_Json_Lookup_Exec HTTP_Log4J_Lookup_Exec HTTP_Log4J_lookup_Suspicious HTTP_Log4J_Post_JndiLdap_Exec HTTP_Log4J_XML_Lookup_Exec	検知可能
	McAfee	・Network Security Platform NS/M Series	HTTP: Apache Log4j2 Remote Code Execution Vulnerability (CVE-2021-44228) [0x4529f700-0]	検知可能
WAF	Imperva	・SecureSphere	CVE-2021-44228: Zero day RCE in Log4j via ldap JNDI parser CVE-2021-44228: Zero day RCE in Log4j via ldap JNDI parser bypass CVE-2021-44228: Zero day RCE in Log4j via ldap JNDI parser bypass 2 CVE-2021-44228 and CVE-2021-45105: Log4J Lookup Infinite Loop CVE-2021-44228: Log4j Java 0-Day Exploit - bypasses to block all - Headers CVE-2021-44228: Log4j Java 0-Day Exploit - bypasses to block all - URL and Param	検知可能
	F5 Networks	・BIG-IP	200104768 JNDI Injection Attempt (Parameter) 200104769 JNDI Injection Attempt (Header)	検知可能
NGFW	Palo Alto	・PA Series	Threat ID 91991, 91994, 91995, 92001, 92004, 92046 Apache Log4j Remote Code Execution Vulnerability	検知可能
	Check Point	・NGFW Series	CPAI-2021-0936 Apache Log4j Remote Code Execution (CVE-2021-44228)	検知可能
総合サーバセキュリティ対策	Trend Micro	・Deep Security	侵入防御 (DPI) ルール 1011242 - Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228) セキュリティログ監視ルール 1011241 - Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	検知可能

Apache Log4j に関する解説

9. 【参考】当社脆弱性検証レポート

   Apache Log4jに存在する RCE 脆弱性(CVE-2021-44228)についての検証レポート

   https://www.intellilink.co.jp/column/vulner/2021/121500.aspx

NTT DATA

Trusted Global Innovator