Distributed via @police
http://www.npa.go.jp/cyberpolice/

平成 27 年 11 月 15 日

Topic

「WebLogic Server」の脆弱性探索が目的と考えられるアクセスの観測について

Java アプリケーションサーバである「WebLogic Server」の脆弱性探索が目的であると考えられるアクセスを観測しました。「WebLogic Server」を利用しているサイト管理者は、速やかな回避策の実施を推奨します。

1 「Apache Commons Collections」と「WebLogic Server」の脆弱性について

「Apache Commons Collections」は The Apache Software Foundation がオープンソースで開発及び公開している Java 言語のライブラリのひとつです。11 月 6 日に、研究者グループから Apache Commons Collections に存在する脆弱性の詳細が公表[i]されました。同脆弱性は既に1月に別の研究者により発表[ii]されていましたが、今回の公表では同ライブラリの脆弱性に起因する複数のソフトウェア群における脆弱性と、具体的な攻撃コードが明らかにされました。また、警察庁では同攻撃コードの内容を元に、脆弱性が存在する複数のソフトウェアをまとめて探索することが可能なツールが公開されていることも確認しています。これを受けて、The Apache Software Foundation も本件について、声明を発表し対応を開始[iii]していますが、15 日 10 時現在では Apache Commons Collections の修正されたバージョンは公開されていません。また、The Apache Software Foundation は今回の問題は Apache Commons Collections に限定されたものではなく、本質的には、認証等を受けておらず信頼のできない相手から受け取ったデータを処理することに問題があるため、プログラムの開発者は、この様な実装を見直すべきであるとしています。

Oracle 社が開発する Java アプリケーションサーバである「WebLogic Server」も、同ライブラリの脆弱性の影響が明らか[iv]にされた製品のひとつです。Oracle 社によると、同脆弱性が悪用された場合には、遠隔からの任意のコードが実行可能となります。

2 「WebLogic Server」の脆弱性探索が目的と考えられるアクセスの観測について

警察庁の定点観測システムにおいては 13 日 18 時から 21 時までの間、攻撃ツールで使用されている固有の文字列が含まれる 7001/TCP に対するアクセスを観測しました（図1）。当該ポートは、WebLogic Server の初期設定で管理コンソールに使用されるポートです。また観測しているリクエストの中に攻撃ツール固有の文字列が含まれていたことから、単に WebLogic Server が稼動しているサーバの探索や、ログインの試行を行うことが目的ではなく、脆弱性が存在するサーバの探索が目的であると考えられます。

このアクセスの発信元 IP アドレスは、サーバのレンタル事業等を行う日本国外の企業が

[i] http://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/
[ii] http://frohoff.github.io/appseccali-marshalling-pickles/
[iii] https://blogs.apache.org/foundation/entry/apache_commons_statement_to_widespread
https://issues.apache.org/jira/browse/COLLECTIONS-580
[iv] 表1を参照。

管理するものでした。探索を実施している者の素性や目的等は不明ですが、この探索に応答を返す WebLogic Server に対しては、さらに当該脆弱性を悪用した攻撃が実施される可能性も考えられます。

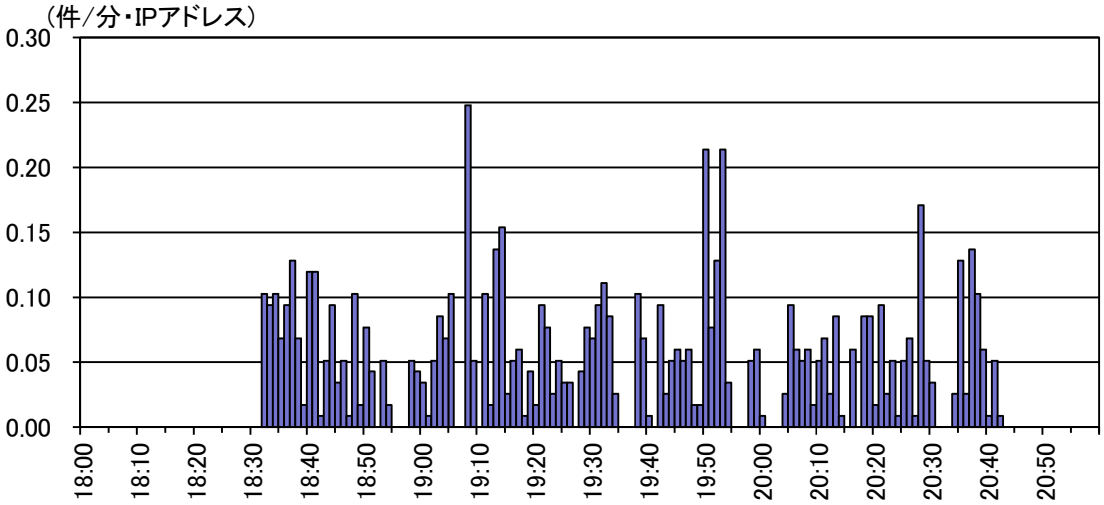

図1 WebLogic Server の脆弱性探索が目的と考えられるアクセス件数の推移
（11 月 13 日 18 時～21 時）

3 推奨する対策

Oracle 社によると、当該脆弱性の影響を受けるバージョンは以下のとおりです。

- Oracle WebLogic Server 10.3.6.0
- Oracle WebLogic Server 12.1.2.0
- Oracle WebLogic Server 12.1.3.0
- Oracle WebLogic Server 12.2.1.0

なお、同社によると当該脆弱性を修正した最新バージョンは準備中[i]であり、15 日 10 時現在ではアップデートは提供されていません。このため、一時的な回避策の実施が推奨[ii]されています。

また、WebLogic Server 以外にも Apache Commons Collections の脆弱性の影響を受けるソフトウェアが多数報告されています。開発元からの脆弱性に関する情報が公表されているものを表1に示します。これらに加えて Apache Commons Collections に起因するものではないものの同様の脆弱性が存在するソフトウェアも明らかとなっています（表2）。これらのソフトウェアを使用している場合には、開発元等が公開する情報を参照して対策を実施することを推奨します。

[i] https://support.oracle.com/rs?type=doc&id=2075927.1 （閲覧にはログインが必要）
[ii] https://support.oracle.com/rs?type=doc&id=2076338.1 （閲覧にはログインが必要）

表1　Apache Commons Collections の脆弱性の影響を受けるソフトウェア

ソフトウェア	開発元による情報
Oracle WebLogic Server	http://www.oracle.com/technetwork/topics/security/alert-cve-2015-4852-2763333.html
Red Hat JBoss	https://access.redhat.com/solutions/2045023
IBM WebSphere Application Server	https://www-304.ibm.com/support/docview.wss?uid=swg21970575
Jenkins	https://jenkins-ci.org/content/mitigating-unauthenticated-remote-code-execution-0-day-jenkins-cli https://wiki.jenkins-ci.org/display/SECURITY/Jenkins+Security+Advisory+2015-11-11
OpenNMS	http://docs.opennms.org/opennms/releases/latest/releasenotes/releasenotes.html#_release_16_0_4

表2　Apache Commons Collections と同様の脆弱性が存在するソフトウェア

ソフトウェア	開発元による情報
Groovy	http://www.groovy-lang.org/security.html
Spring	https://jira.spring.io/browse/SPR-13656

さらに、Java 言語を使用して、独自のソフトウェアを開発及び運用している場合についても、これらの脆弱性の影響を受ける可能性があります。このため、開発者やサーバ管理者にあっては、開発しているソフトウェア及び運用しているサーバの実行環境について確認を実施することを推奨します。