— AUS（アルテミス・ユーザ・サポート）便り 2021/12/14号 —
https://www.artemis-jp.com

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●Log4jに致命的な脆弱性…至急アップデート・回避策実施を

https://www.jpcert.or.jp/at/2021/at210050.html
https://www.itmedia.co.jp/news/articles/2112/10/news157.html

このニュースをザックリ言うと･･･

- 12月10日(日本時間)、Javaプラットフォームでのログ取得用ライブラリ「Apache Log4j」のバージョン2(Log4j2)において非常に危険度が高いとされる脆弱性の存在が明らかとなり、修正バージョン2.15.0がリリースされています。

- 脆弱性はLog4j2の「JNDI Lookup」という機能によるもので、Log4j2が組み込まれたJavaアプリケーションが処理するログに特定の文字列が含まれるとき、同一コンピューター上あるいは外部サーバー上にあるJavaバイナリファイル(class)をダウンロードし、最悪の場合任意のコードをソフトウェア上で実行される恐れがあるとされています。

- 同11日にはJPCERT/CC等でも注意喚起が出されており、Log4j2(バージョン2.0.0～2.14.1)を利用している全てのケースでアップデートか、JDNI Lookupを無効化する回避策の実施が必須とされています。

AUS便りからの所感等

- 人気ゲームソフト「Minecraft」のJava EditionにLog4j2が含まれており、ゲームサーバーにログインした攻撃者が悪用するケースが報告されたことが脆弱性を広く知らしめる一因となりましたが、これ以外にもJavaで実装され、Log4j2を含むアプリケーションは非常に多く、かつ攻撃が比較的容易とされることから、2014年に話題になった「Heartbleed」「Shellshock」と同等あるいはそれ以上の危険度の脆弱性とされています。

- 脆弱性について最も想像しやすいケースは、WebアプリケーションをJavaで実装している場合に、細工したリクエストをWebサーバーからアプリケーションへ渡すケースが挙げられますが、攻撃経路はHTTPリクエストとは限りませんし、また内部からのファイルのダウンロードでLDAPが使用されるケースが主に紹介されているものの、やはりそれに限定されるものではないでしょう。

- Webサーバー等、インターネットと直接繋がっているサーバー上のアプリケーションでJavaを使用していなくても、より内部のサーバーにあるJavaアプリケーションと通信している場合、さらにはクライアントアプリケーションが外部のサーバーとのやり取りで不正なデータを送り込まれた場合にも、アプリケーションを踏み台にして内外のサーバーへの通信等が行われる恐れがあります。

- 既にクラウドサービスやセキュリティベンダー各社が提供するWAFでは攻撃パターンを遮断する設定を追加したと発表されていますが、より複雑なリクエスト等でWAFを回避される可能性も指摘されており、根本的対策のため、Javaアプリケーションが使用されている箇所を全て洗い出し、それぞれLog4j2のアップデート、もしくはそれが実行できない場合は回避策を実行するよう徹底してください。

- 加えて、Log2jについて対策できたか否かに拘わらず、サーバーOSの設定あるいはその前面にUTMを設置する等により、サーバー自身からの外部への意図しない通信を遮断する「出口対策」をとることを推奨致します。

JPCERT CC
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

Apache Log4jの任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起
最終更新: 2021-12-13

Javaベースのオープンソースのロギングライブラリの Apache Log4j には、任意のコード実行の脆弱性（CVE-2021-44228）があります。
Apache Log4j が動作するサーバーにおいて、遠隔の第三者が本脆弱性を悪用する細工したデータを送信することで、任意のコードを実行する可能性があります。

IV. 回避策

The Apache Software Foundationから、Log4jのバージョンに応じた回避策に関する情報が公開されています。

Log4jバージョン2.10及びそれ以降
- 次のいずれかを実施する
（1）Log4jを実行するJava仮想マシンを起動時に「log4j2.formatMsgNoLookups」というJVMフラグオプションを「true」に指定する 例: -Dlog4j2.formatMsgNoLookups=true
（2）環境変数「LOG4J_FORMAT_MSG_NO_LOOKUPS」を「true」に設定する

Log4jバージョン2.10より前
- JndiLookupクラスをクラスパスから削除する

●医薬品メーカーから個人情報のべ22万件流出か…国内外拠点サーバーに不正アクセス

https://www.itmedia.co.jp/news/articles/2112/06/news156.html
https://www.release.tdnet.info/inbs/140120211206447090.pdf

このニュースをザックリ言うと･･･

－ 12月6日(日本時間)、医薬品メーカーのリニカル社より、同社サーバーが不正アクセスを受け、個人情報が流出したと発表されました。

－ 発表によれば、対象となる情報は、採用応募者情報約14,000件、2015年3月31日～2021年6月30日の間に株主名簿上に記載があった個人株主約21,000件、2009年3月31日～2014年12月31日の同名簿上に情報があった個人株主約60,000件(のべ件数)、取引先の社員個人情報約30,000件等、のべ22万件にのぼるとされています(臨床試験の被験者データはクラウドサーバー上の別環境にあり、影響は受けていないとのことです)。

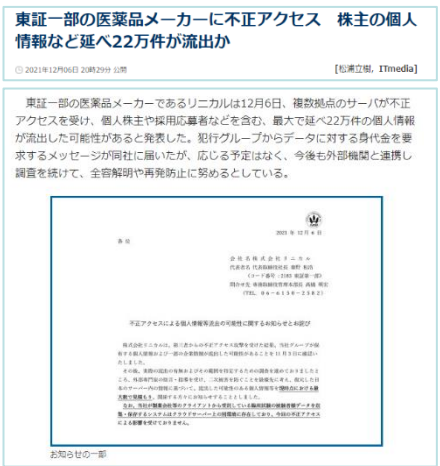
－ 同社からは10月5日の時点で、同3日に不正アクセスが確認されたことが発表されており、その後日本本社・台湾拠点および欧州拠点のサーバーが不正アクセスを受けたこと等が明らかになっています(同27日には欧州拠点への攻撃に関連してサイバー犯罪グループ「RAGNAR LOCKER」から脅迫メッセージが送られていたことが発表されています)。

AUS便りからの所感

－ 同社では「ID・パスワード管理の手順化と周知徹底」「多重認証システムを導入」「不正アクセス防止・検知を行うセキュリティソフトウエアと、侵入後の検知・分析を行うEDR(Endpoint Detection and Response)サービスを導入」等の対策、そして「サイバーセキュリティ保険への加入」を行っていたとしており、社内PCやメールサーバーへのマルウェア感染被害はなく、現時点では被害を受けたサーバーも復旧しているとのことです。

－ 侵入経路となったのはVPN装置の脆弱性とされ、これも同社では対策済みとしていますが、近年VPN装置に対する攻撃が多発し、対策を行うようメーカーからも注意喚起が出されていた中、1つでも侵入可能な拠点があったことにより、このような大規模な個人情報の流出に繋がったことは痛恨と言えます。

－ とにかく全ての拠点で利用しているあらゆるネットワーク機器について確実に捕捉・管理し、脆弱性の対策を随時行えるような体制、またUTMの設置等により、(同社でも行っているとする)不正アクセスの検知・情報流出の遮断を行う体制を整え、「蟻の一穴」からのセキュリティ侵害を食い止められるようにすることが肝要です。


ITmedia NEWS

東証一部の医薬品メーカーに不正アクセス　株主の個人情報など延べ22万件が流出か

2021年12月06日 20時29分 公開　[松浦立樹, ITmedia]

東証一部の医薬品メーカーであるリニカルは12月6日、複数拠点のサーバが不正アクセスを受け、個人株主や採用応募者などを含む、最大で延べ22万件の個人情報が流出した可能性があると発表した。犯行グループからデータに対する身代金を要求するメッセージが同社に届いたが、応じる予定はなく、今後も外部機関と連携し調査を続けて、全容解明や再発防止に努めるとしている。

不正アクセスによる個人情報等流出の可能性に関するお知らせとお詫び

お知らせの一部

●LINE Pay決済情報約13万人分がGitHubで公開状態に…グループ会社従業員が無断でアップロード

https://www.itmedia.co.jp/news/articles/2112/06/news162.html
https://linecorp.com/ja/pr/news/ja/2021/4032

このニュースをザックリ言うと･･･

－ 12月6日(日本時間)、LINE Pay社より、同社運営の「LINE Pay」による決済情報の一部がソースコード共有サイト「GitHub」上で閲覧できる状態になっていたと発表されました。

－ 発表によれば、対象となる情報は2020年12月26日～2021年4月2日に行われた決済に関する133,484アカウント(うち国内ユーザー51,543アカウント)分の、アプリ内でのID・加盟店管理番号・キャンペーン情報(決済金額・日時が含まれる場合ありとのこと)とされ、氏名・住所・電話番号・メールアドレス・クレジットカード番号・銀行口座番号等は含まれていないとのことです。

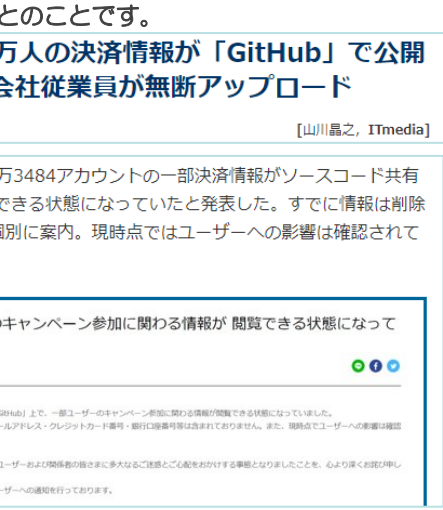
－ GitHubに公開されていたのは9月12日～11月24日で、11月24日に社内モニタリングによる発見・削除までに部外者からのアクセスが11件あったとされていますが、現時点でユーザーへの影響は確認されていないとのことです。

AUS便りからの所感

－ 同社委託先のグループ会社従業員がポイント付与漏れの調査を行っていた際、調査プログラムとともに誤って決済情報の一部をアップロードし、公開状態としていたことが原因とされています。

－ 発表された範囲では、不正ログインに繋がり得る情報や、前述のように個人情報そのものが流出した様子はなく、現時点では深刻な流出事故とは言えないようですが、万が一アプリ内で使用されるIDでなりすましやリンクされているユーザー個人へ繋がり得る手法が発見される可能性は理論上考えられます。

－ ともあれ現時点で問われるべきは、今年1月に大手企業複数社のシステムに関連するとみられるソースコードがGitHubにアップロードされる事態が発生した(AUS便り 2021/02/08号参照)時と同様、「GitHubを使っていたこと」ではなく、「適切な使い方に関する教育が十分だったか」等と言えるでしょう。


ITmedia NEWS

LINE Pay、約13万人の決済情報が「GitHub」で公開状態に　グループ会社従業員が無断アップロード

2021年12月06日 21時31分 公開　[山川晶之, ITmedia]

LINE Payは12月6日、13万3484アカウントの一部決済情報がソースコード共有サイト「GitHub」上で閲覧できる状態になっていたと発表した。すでに情報は削除しており、該当ユーザーへ個別に案内。現時点ではユーザーへの影響は確認されていないという。

【LINE Pay】一部ユーザーのキャンペーン参加に関わる情報が 閲覧できる状態になっていた件のお知らせとお詫び

2021.12.06 / Fintech関連サービス

このたび、ソフトウェア開発のプラットフォームである「GitHub」上で、一部ユーザーのキャンペーン参加に関わる情報が閲覧できる状態になっていました。
閲覧可能となっていた情報に、氏名・住所・電話番号・メールアドレス・クレジットカード番号・銀行口座番号等は含まれておりません。また、現時点でユーザーへの影響は確認されておりません。

本件につきまして、下記の通り報告いたしますとともに、ユーザーおよび関係者の皆さまに多大なるご迷惑とご心配をおかけする事態となりましたことを、心より深くお詫び申し上げます。
現在、閲覧できる状態にあった当該情報は削除し、該当ユーザーへの通知を行っております。