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。

●さらなるLog4jのセキュリティアップデート…一部回避策は非推奨、1.17.0へ更新か該当機能削除を

https://forest.watch.impress.co.jp/docs/news/1374095.html
https://forest.watch.impress.co.jp/docs/news/1375445.html
https://www.jpcert.or.jp/at/2021/at210050.html

このニュースをザックリ言うと･･･

- 12月14日および18日(いずれも日本時間)、 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、新たな脆弱性に対応した修正バージョンが相次いでリリースされています。

- Log4j2は同10日に任意のコードを実行可能な脆弱性「CVE-2021-44228(別名Log4Shell)」を修正するバージョン2.15.0がリリース(AUS便り 2021/12/14号参照)されましたが、その後14日に、同様の脆弱性である「CVE-2021-45046」を修正するバージョン2.16.0が、さらに18日には、Javaアプリケーションを強制終了させる、いわゆるサービス拒否(DoS)攻撃に繋がる脆弱性「CVE-2021-45105」を修正するバージョン2.17.0がリリースされています。

- Log4j2(バージョン2.0.0～2.16.0)を利用している全てのケースで、2.17.0へのアップデート、またはアップデートできない場合は回避策の実施が必須とされていますが、2.15.0リリース時点で挙げられていた回避策では全ての脆弱性に対応できない場合があるとして推奨されておらず、別の回避策が挙げられています。

AUS便りからの所感等

- Java 7を使用している古いシステムでは2.15.0以降へアップデートできないため、対応バージョンである2.12.2がリリースされています(ただしCVE-2021-45105は未修正で、2.12.3で対応予定とのことです)。

- アップデートできない場合の回避策として、脆弱性の原因となる「JNDI Lookup」に関連するファイル(Jndilookup.class)をclasspathから削除することが挙げられていますが、(以前推奨されていた)コマンドラインオプションの追加等に比べ取り扱いが難しい場合があり、適切に動作するか確認すべきでしょう。

- Log4Shellの発表と前後して脆弱性を悪用する攻撃が多数報告されていますので、インターネット上のサーバーから社内のサーバー・クライアントPCまで、Javaアプリケーションないし Log4jが使用されている箇所の洗い出しとLog4j2のアップデート等による根本的対策を今一度呼び掛けるとともに、OSの設定やUTMの設置等による脆弱性侵害時の「出口対策」も併せて検討して頂ければ幸いです。

Impress Watch

「Apache Log4j」に3つ目の脆弱性 ～修正版のv2.17.0が公開

「Log4j 2.15.0」のLog4Shell対策に漏れ、DoS攻撃を受ける可能性

樽井 秀人　2021年12月20日 10:16

Apacheソフトウエア財団、「Apache Log4j 2.17.0」をリリース

The Apache Software Foundation（ASF）は12月17、ロギングライブラリ「Apache Log4j 2.17.0」をリリースした。新たな脆弱性「CVE-2021-45105」が発見されたとして、その修正が行われている。

開発チームによると、JNDI LDAPルックアップ機能に起因するリモートコード実行の脆弱性（CVE-2021-44228、通称：Log4Shell）を緩和するため、「Log4j 2.15.0」ではJNDI LDAPルックアップ機能をlocalhostに限定する対策が導入されている。しかし、ログ設定でコンテキストルックアップを含むデフォルト以外のパターンレイアウト（例：$${ctx:loginId}）を使用している場合、攻撃者は再帰的なルックアップを引き起こす悪意ある入力データを作成できる。これはスタックオーバーフローエラーを引き起こしてプロセスを終了させるサービス拒否（DoS）攻撃につながりうる。

● EMOTETが悪用する脆弱性も…MS12月月例セキュリティパッチ

https://cloud.watch.impress.co.jp/docs/news/1374347.html
https://msrc-blog.microsoft.com/2021/12/14/202112-security-updates/
https://www.jpcert.or.jp/at/2021/at210051.html
https://www.ipa.go.jp/security/ciadr/vul/20211215-ms.html

このニュースをザックリ言うと・・・

- 12月15日(日本時間)、マイクロソフト(以下・MS)より、月例のセキュリティパッチ(Windows 10向けパッチKB5008212他)がリリースされ、多数の脆弱性が修正されています。

- 修正された脆弱性のうち、Windows AppX installerにおけるなりすましの脆弱性「CVE-2021-43890」について、11月に活動再開したとみられているマルウェア「Emotet」(AUS便り 2021/11/24号参照)による悪用の事実を確認済みであることがMSから発表されています。

- この他、暗号化ファイルシステム(EFS)をネットワーク上で利用するケースで発生する脆弱性等の修正も含まれており、同日、JPCERT/CC・IPAからもセキュリティアップデートを早急に適用するよう注意喚起が出されています。

AUS便りからの所感

- Windows 10 バージョン2004については、今回が最後のセキュリティパッチリリースとなるため、以後は最新バージョン21H2等へのアップグレードを行うようにしてください。

- Windows10におけるセキュリティパッチには最近でも度々不具合の発生が報告されていますが、だからといって安易にパッチをアンインストールすることは、他の脆弱性への対策も無効になる恐れがあり危険なため、基本的にはアップデートを行うようにし、またシステム管理者等においても組織内で問題が発生していないか調査するとともに、回避策があるか情報収集と提供を行うこと、またパッチ未適用状態のPC等が攻撃を受ける可能性を抑止するため、アンチウイルスやUTMによる防御を確実に行う体制を整えることが肝要です。

Impress Watch

Microsoftが12月の月例パッチ公開、「Windows 10 バージョン2004」はサポート終了

三柳 英樹　2021年12月15日 11:58

日本マイクロソフト株式会社は15日、12月の月例セキュリティ更新プログラム（修正パッチ）を公開した。マイクロソフトではユーザーに対して、できるだけ早期に修正パッチを適用するよう呼びかけている。

対象となるソフトウェアは、Windows、Office、SharePoint、ASP.NET Core、Visual Studio、Microsoft Defender for IoT、PowerShell。

これらのうち、最大深刻度が4段階で最も高い"緊急"の脆弱性の修正が含まれるソフトウェアは、Windows（Windows 11/10/8.1、Windows Server 2022/2019/2016/2012 R2/2012）、Office、Visual Studio、Microsoft Defender for IoT。修正パッチに含まれる脆弱性の件数はCVE番号ベースで67件で、うち最大深刻度が"緊急"のものが7件。また、Microsoft Edgeについては、月例の修正パッチとは別のタイミングでアップデートが行われている。

●年末年始における情報セキュリティに関する注意喚起、IPAより発表

https://www.ipa.go.jp/security/topics/alert20211216.html

このニュースをザックリ言うと・・・

- 多くの企業が長期休暇となる年末年始を迎えるにあたり、12月16日(日本時間)にIPAより、情報セキュリティに関する注意喚起が出されています。

- システム管理者が長期間不在になる等により、ウイルス感染や不正アクセス等のインシデント発生に気付きにくく対処が遅れてしまう可能性、および従業員等が友人や家族と旅行に出かけた際の、SNSへの書き込み内容から思わぬ被害が発生、場合によっては関係者にも被害が及ぶ可能性を指摘しています。

- JPCERT/CCや内閣官房内閣サイバーセキュリティセンター(NISC)等からも同様の注意喚起が出る可能性があり、内容を確認の上、休暇に備えることが推奨されます。

AUS便りからの所感

- IPAは毎年のこの時期あるいはゴールデンウィークや夏季休暇の時期に注意喚起を行っており(https://www.ipa.go.jp/security/measures/vacation.html)、今回についてはマルウェア「Emotet」への注意がトピックとして挙げられている他、相談事例として「通信事業者を装った偽SMS」「メールサービス事業者を装ったフィッシングメール」についても取り上げられ、やはり注意が促されています。

- こういったセキュリティ機関の呼びかけでは、組織内のシステム管理者やユーザに対し、休暇前・休暇中および休暇明けにとるべき対策のポイントが挙げられており、情報システムとインターネットを組織内外で利用する者として、「普段から」セキュリティを意識した慎重な行動をとることを改めて示す以外にも、「いつもとは違う状況になる」ことで通常時には生じにくい様々な問題にも早く確実に対応することへの注意を促すものとなっています。

- 注意喚起等を年明け以降にご覧になったとしても、その時点で点検すべきことは様々ですので、以後も、ゴールデンウィークや夏季といった長期休暇に備えて、準備・点検を行うよう意識して頂ければ幸いです。

IPA

年末年始における情報セキュリティに関する注意喚起

最終更新日：2021年12月16日
独立行政法人情報処理推進機構
セキュリティセンター

多くの人が年末年始の長期休暇を取得する時期を迎えるにあたり、IPAが公開している長期休暇における情報セキュリティ対策をご案内します。

長期休暇の時期は、「システム管理者が長期間不在になる」、「友人や家族と旅行に出かける」等、いつもとは違う状況になりがちです。このような場合、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまったり、SNSへの書き込み内容から思わぬ被害が発生したり、場合によっては関係者に対して被害が及ぶ可能性があります。

最近では外出自粛等の影響により、従来オフィスで利用していたパソコンなどを利用する時間が長くなり、ウイルス感染やネット詐欺被害のリスクが高まることも考えられます。

これらのような事態とならないよう、(1)組織のシステム管理者、(2)組織の利用者、(3)家庭の利用者、のそれぞれの対象者に対して取るべき対策をまとめています。

■長期休暇における情報セキュリティ対策

また、長期休暇に限らず、日常的に行うべき情報セキュリティ対策も公開しています。

■日常的に実施すべき情報セキュリティ対策

被害に遭わないためにもこれらの対策の実施をお願いします。

2021年11月から「Emotet」（エモテット）と呼ばれるウイルスの攻撃活動が再開し、12月現在も攻撃が継続しています。IPAの相談窓口でも感染の可能性がある相談を、12月に入ってから数件確認しています。再び被害が拡大していく可能性があり、改めて注意いただくようお願いします。

Emotetの攻撃では、過去にやり取りされたメールが攻撃者に盗まれ、その内容やメールアドレスが転用されて、ウイルスメールとして送られてくることがあります。
顧客や取引先、知人からのメールに見えても、すぐに添付ファイルやURLリンクは開かず、本物のメールであるか落ち着いて確認してください。
長期休暇明けはメールが溜まっていることが想定されますので、一件一件の確認を慎重に行ってください。

■「Emotet」と呼ばれるウイルスへの感染を狙うメールについて