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。

●Apache 2.4.49～2.4.50に脆弱性、アップデート二度リリース…利用者は2.4.51へ更新を

https://news.mynavi.jp/article/20211006-2008922/
https://news.mynavi.jp/article/20211008-2036410/

このニュースをザックリ言うと・・・

- 10月4日(現地時間)、Webサーバーソフトウェア「Apache HTTP Server(以下・Apache)」の開発元より、Apacheバージョン2.4.49に2件の脆弱性が確認されたとして、アップデートバージョン2.4.50がリリースされました。

- 修正された脆弱性のうち1件(CVE-2021-41773)は、Apacheの設定次第で、サーバー上の任意の場所にあるファイルが取得可能になる恐れがあり、既に悪用が確認されているとのことです。

- しかし同7日、当該脆弱性の修正が不十分で、別の方法で同様の攻撃が可能(CVE-2021-42013)であることが明らかになり、さらなるアップデートバージョン2.4.51がリリースされています。

AUS便りからの所感等

- 問題となっている脆弱性は「ディレクトリトラバーサル」と呼ばれ、ファイルの場所を示す等のリクエストパラメータに不正な記号を含むことにより、本来意図されていない外部ディレクトリへの参照を行うというものです。

- 2000年にマイクロソフト製WebサーバーのIISにおいてこの脆弱性が発見され、修正される等、クロスサイトスクリプティング(XSS)等と並ぶ古典的なものであり、またWebアプリケーション側でパラメータのチェック不足によって起こるケースも多く、不正アクセスによる情報流出の原因となることも度々あります。

- 今回の脆弱性は9月にリリースされたApache 2.4.49～2.4.50でのみ存在するもので、例えばCentOS・Debianといったディストリビューションのパッケージからインストールしている場合には、まだこのバージョンを使っていないため影響は受けないとされていますが、一方で独自にソースコードからインストールを行った場合や、Windows向けバイナリ等で2.4.49以降を導入している場合は、必ず2.4.51へのアップデートを行うようにしてください。

- また、脆弱性を悪用する不正なリクエストを遮断するよう、Webアプリケーションファイアウォール(WAF)の導入も、可能であれば検討するのが良いでしょう。

TECHR Powered by マイナビニュース


Apache HTTP Server 2.4.50リリース、ゼロデイ脆弱性の修正も

Apache Software Foundationは10月4日(米国時間)、「Apache HTTP Server 2.4.50 Released - The Apache HTTP Server Project」において、オープンソースのWebサーバソフトウェア「Apache HTTP Server 2.4.50」をリリースしたと伝えた。このリリースには2件の脆弱性の修正が含まれており、そのうちの1件はすでに攻撃への悪用が確認されているゼロデイ脆弱性に該当する。

Apache HTTP SERVER PROJECT

Apache HTTP Server 2.4.50 Released

October 04, 2021

The Apache Software Foundation and the Apache HTTP Server Project are pleased to announce the release of version 2.4.50 of the Apache HTTP Server ("Apache"). This version of Apache is our latest GA release of the new generation 2.4.x branch of Apache HTTPD and represents fifteen years of innovation by the project, and is recommended over all previous releases. This release of Apache is a security, feature and bug fix release.

We consider this release to be the best version of Apache available, and encourage users of all prior versions to upgrade.

Apache HTTP Server 2.4.50 is available for download from:

https://httpd.apache.org/download.cgi


Apache HTTP Server 2.4.51リリース、2.4.50の修正では不十分と判明

米コンピュータ緊急事態対策チーム（US-CERT）United States Computer Emergency Readiness Team）は10月7日(米国時間)、「Apache Releases HTTP Server version 2.4.51 to Address Vulnerabilities Under Exploitation （CISA）」において、Apache Software Foundationがオープンソースのwebサーバソフトウェア「Apache HTTP Server 2.4.51」をリリースしたと伝えた。このリリースでは、すでに悪用が確認されているパストラバーサルのゼロデイ脆弱性に対する修正が含まれている。

該当する脆弱性に関する情報は次の脆弱性情報ページにまとめられている。

- Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project

Fixed in Apache HTTP Server 2.4.51

critical: Path Traversal and Remote Code Execution in Apache HTTP Server 2.4.49 and 2.4.50 (incomplete fix of CVE-2021-41773) (CVE-2021-42013)

●「Windows 11」システム要件を満たすデバイス、半数未満

https://news.mynavi.jp/article/20211006-2007007/
https://www.lansweeper.com/itam/is-your-business-ready-for-windows-11/

このニュースをザックリ言うと･･･

- 9月28日(現地時間)、IT資産管理ソリューションを提供するLansweeper社より、約6万組織・約3,000万台のWindowsデバイスについて、10月5日にリリースされた「Windows 11」のシステム要件を満たしているか調査を行った結果が発表されました。

- 調査によれば、3つの主なシステム要件のうち、対応率が最も低かったのがCPUの要件(周波数1GHz以上、コア数2以上の64ビットCPU等)で、満たしているデバイスは44.4%に留まっています。

- また、メモリの要件(4GB)は91.05%が満たしている一方で、Trusted Platform Module(TPM)2.0への対応が確認されたデバイスも52.55%程度(この他28.19%がTPMと互換性がないまたは有効にされていない)とされています。

AUS便りからの所感

- マイクロソフトでは、システム要件を満たさないデバイスに手動でWindows 11をインストールすること自体は可能なものの、更新プログラムの配布は保証しないとしており、セキュリティパッチが適用されない状態となる可能性があります。

- 現行のWindows 10の一般ユーザー向けサポートは2025年10月までとなっており、それまでの約4年間において、要件を満たしていないPC等のリプレースを確実に行うよう、早期に計画を立てることを推奨致します(なお半年ごとのバージョンリリースについて、バージョン2004のサポートが12月で終了となるため、20H2以降へのアップデートができないPCがある場合もリプレースが必要です)。

- 要件を満たすPCにおいて、Windows Updateから、11へのアップグレードが可能であることを示すメッセージが出ることがありますが、リリースされたばかりで不安定な面があることが報告されているため、組織内のPCで勝手にアップグレードを行わないよう管理者から呼び掛ける等の対応も適宜必要となるでしょう。

●9月度フィッシング報告数は49,953件…依然5万件に近い高水準

https://www.antiphishing.jp/report/monthly/202109.html

このニュースをザックリ言うと･･･

- 10月5日、フィッシング対策協議会より、9月に寄せられたフィッシング報告状況が発表されました。

- 9月度の報告件数は49,953件で、8月度(https://www.antiphishing.jp/report/monthly/202108.html)の53,177件からは3,224件減少となっており、またフィッシングサイトのURL件数が6,636件(8月度9,024件)、悪用されたブランドが件数76件(8月度89件)となっています。

- 報告全体に対するブランドの割合については、最も多いAmazonは30.6%と8月度(24.8%)より増加、これにETC利用照会サービス・イオンカード・三井住友カード・厚生労働省のコロナワクチンナビを合わせた5ブランドで約64.0%(8月度 65.8%)、また1,000件以上の報告があったブランドが10あり、これらで全体の約81.6%を占めたとしています。

AUS便りからの所感

フィッシング対策協議会
Council of Anti-Phishing Japan

- 過去最多を記録した8月度よりは減少したものの、歴代2位の報告件数となっており、10月度も5万件前後で推移するかは不透明なものの、少なくとも2020年10月度以降の「1年間連続で3万件以上」を維持することは確実でしょう。

- 前述したブランド以外でも、NTTドコモから同社を騙るSMSによるフィッシング詐欺で1億円の被害が出たことが発表(AUS便り2021/10/05号)、対策協議会からはさくらインターネット・お名前.comといったインターネットサービスを騙るフィッシングについて注意喚起が出ている等、フィッシングの攻撃範囲は多岐にわたっています。

- 同協議会では、メール文面に違和感のない見破ることが困難なフィッシングメールでも、送信元IPアドレスのSPFによる検証、送信元メールアドレスのDMARCによる検証および従来から使われている迷惑メールフィルターとの組合せにより、検出できるケースが多いとしており、メールサーバー等におけるこういった機構の導入や、各種機構に対応しているメールサービスの利用の検討は、自組織のユーザーの保護、あるいは顧客ユーザー等を保護する観点からも重要と言えるでしょう。