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。

●PHPの致命的な脆弱点「php2shell」で緊急パッチリリース、アップデート等のため休止のWebサイトも



https://www.jpcert.or.jp/at/2026/at260033.html
https://www.php.net/archive/2026.php#2026-10-21-5

このニュースをザックリ言うと・・・

- 10月21日(日本時間)、プログラミング言語および処理系PHPの開発元より、PHPにおいて2件の危険度の高い脆弱点「php2shell」(CVE-2026-109618, CVE-2026-109619)が存在することが発表され、同日23時に修正バージョン(8.5.12・8.4.27・8.3.36・8.2.35)がリリースされました。

- 脆弱点は主にmultipartリクエスト(Webからのファイルアップロード時に使用)の処理時に発現し、リモートからPHPが導入されているサーバーを乗っ取られる恐れがあるものとされており、また修正バージョンのリリース前に脆弱点の詳細が第三者によって公表され、攻撃コードも出回る等の事態が発生していました。

- また各種Linuxディストリビューション(RHELおよびAlmalinux・Rocke Linux等の派生、Debian・Ubuntu等)においても、修正パッケージが極めて迅速にリリースされる異例の対応が行われています。

- 開発元ではすぐにセキュリティアップデートが適用できない場合の緩和策として、php.iniにて「session.upload_progress.enabled=0」の設定を行うことを推奨しています。

AUS便りからの所感等

- 今回日本国内でもPHPで構築されていたとみられる大手Webサービスや、PHPを提供するホスティングサービスにおいて大規模なメンテナンスが順次実施され、これらの中には対応完了までサービスを休止した事例も多くみられており、「機会損失の可能性があったとしても脆弱性対応のためにサービスの休止を行う」という選択肢も今後より現実的になってくるものとみられます。

- 同23日には同様の脆弱点(CVE-2026-115560)の存在も開発元から発表されましたが、影響を受ける環境は限定的とされることから修正は後日行われる予定で、前述した緩和策の設定がここでも有効になるとされています。

- 奇しくもNode.JSやApache Tomcat、またはRubyやPythonといった、PHPと同様にWebアプリケーションの基盤となっている他のソフトウェアでも相次いで脆弱点が発表され、セキュリティアップデートがリリースされましたが、危険度の高低こそあれこのようなセキュリティアップデートはどのソフトウェアでも常時発生するものであり、例えば「PHPそのものの使用を避ける」みたいな判断を安易にとるのではなく、管理者においては使用している全てのソフトウェアについて常に最新のバージョンに保つ体制を維持することが肝要と言えます。



●SSL中間証明書で脆弱な鍵の使用が発覚、Webブラウザー以外にも影響あり

https://internet.watch.impress.co.jp/docs/news/2150339.html
https://emudhra.com/en/post/certificate-security-incident
https://forest.watch.impress.co.jp/docs/serial/yajiuma/2150316.html



このニュースをザックリ言うと・・・

- 10月20日(現地時間)、インドの認証局eMudhra社より、同社によるSSLサーバー証明書等の発行・証明用として計8つの脆弱な中間証明書を作成していたと発表されました。

- 問題となった中間証明書は楕円曲線暗号(ECC)を用いた証明書用のもので、秘密鍵として4～237という極めて小さな整数を使用しており、容易に推測が可能だったとしています。

- Firefoxブラウザーを開発するMozilla Foundationが報告を受けて情報を公開し、該当する中間証明書はeMudhraによって失効(revoke)され、Microsoft・Google・Apple等OS・ブラウザーベンダー各社においても無効化等の対応をとっています。

AUS便りからの所感

- eMudhraでは、中間証明書の署名を行うキーセレモニーの際に手違いで脆弱な秘密鍵が生成・使用されたとしています。

- 推測された秘密鍵を悪用して発行されたサーバー証明書は、対策が行われていないブラウザーやOS等から理論上正規の証明書と認識される可能性があり、正規のサーバーとの通信を盗聴・改ざんするための不正なサーバーやWi-Fiアクセスポイント等を設置するといった攻撃が行われる恐れがあったとみられます。

- 報告を行った研究者により、ブラウザー等が問題のある証明書が有効でないかチェックするためのサイト(https://emudhra.we-have-a-problem.com/)が用意されており、少なくとも手元のブラウザーを最新にアップデートした後、当該サイトにアクセスの上「接続されませんでした」と表示されるか確認することが推奨されます。

- WebブラウザーやOS以外のソフトウェア、こと外部とWebアクセスや暗号化通信を行うものについてはもちろん、一見ネットワーク機能を持っていないようなものでもWebブラウザーのエンジンを組み込んでいるものについては今回の問題に影響する可能性があり、これを受けてアップデートが行われたものについては一通り対応を行うべきです。


インドの認証局eMudhraで秘密鍵の欠陥が明らかに。ユーザーができる対策はOSやブラウザーのアップデート

山田 貞幸　2026年10月22日 13:36

eMudhra Statement on Recent Certificate Security Incident

eMudhra Statement on Recent Certificate Security Incident（eMudhra）より1

インドの認証局（CA：Certificate Authority）であるeMudhraで、公開鍵暗号の証明書（中間証明書）の一部において極めて短い桁数の秘密鍵が使われ、容易に割り出される状態になっていたことが明らかになり、実際の秘密鍵も漏えいした。

公開鍵暗号はインターネットにおいて広く使われているプロトコル「HTTPS」における暗号化などに取り入れられている技術であり、その秘密鍵が漏えいしたことは、悪意のある攻撃者が偽の証明書を発行するなど、インターネットにおける秘密の保持や安全性の維持において、深刻な影響を与える。

●ターゲット個人に特化したフィッシングメールをAIで生成→クリック率上昇との研究結果

https://www.itmedia.co.jp/news/article/2610/27/2000002550/



このニュースをザックリ言うと・・・

- 10月27日(日本時間)、ITMediaにて、送信相手に特化した文面のフィッシングメールを用いる「スピアフィッシング」についての実験を基にした海外の論文が取り上げられています。

- 論文はドイツのベルリン工科大学等の研究者らによるもので、実験では対象となる大学職員についての公開情報をサーチエンジンで抽出し、複数のAIモデルによってプロファイリングを行った上で、3,310人に対し最適な差出人と文面を自動生成したフィッシングメールを送信したとしています。

- 結果、全員に共通の文面を送る一般的なフィッシングメールのクリック率が3.9%なのに対し、相手に特化した文面のAI生成メールではクリック率が10%に上昇したとのことです。

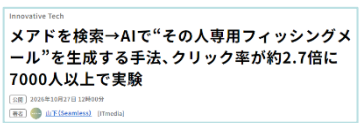
- またAI生成のメールを大学のフィルターにかけた場合、3,949通のうち不審なものと判定されたのは1通のみだったとしています。

AUS便りからの所感

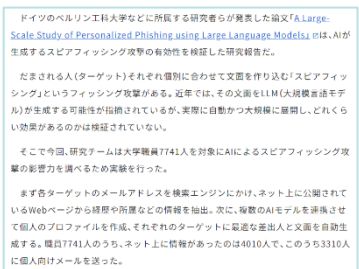
- 専門家が手作業で作成したフィッシングメールのクリック率は24.2%であるものの、AIによる生成メールは約4,000通を約50時間で作成する等、効率面で優位ともしています。

- 10月19日にフィッシング対策協議会から発表された9月のフィッシング報告状況(https://www.antiphishing.jp/report/monthly/202609.html)においてもフィッシングメールに受信者の氏名が記載されているケースがみられたとしており、9月以降に多発した情報漏洩事案との関連が指摘されています。

- フィッシング回避のための「不審なメールのリンクは開かない」という大前提もAI生成の巧妙な文面で破られる可能性もあり、コンテンツベースの迷惑メールフィルターあるいはSPF・DKIM・DMARCによるなりすまし検知機構も完璧とは言えず、これらを組合せ、さらには相手に別の経路で確認する等により、正しいメールか否かを判断する精度を上げることを心掛けるべきでしょう。


Innovative Tech

メアドを検索→AIで“その人専用フィッシングメール”を生成する手法、クリック率が約2.7倍に 7000人以上で実験


ドイツのベルリン工科大学などに所属する研究者らが発表した論文「A Large-Scale Study of Personalized Phishing using Large Language Models」では、AIが生成するスピアフィッシング攻撃の有効性を検証した研究報告だ。

だまされる人（ターゲット）それぞれ個別に合わせて文面を作り込む「スピアフィッシング」というフィッシング攻撃がある。近年では、その文面をLLM（大規模言語モデル）が生成する可能性が指摘されているが、実際に自動かつ大規模に展開し、どれくらい効果があるのかは検証されていない。

そこで今回、研究チームは大学職員7741人を対象にAIによるスピアフィッシング攻撃の影響力を調べるため実験を行った。

まず各ターゲットのメールアドレスを検索エンジンにかけ、ネット上に公開されているWebページから経歴や所属などの情報を抽出。次に、複数のAIモデルを連携させて個人のプロファイルを作成、それぞれのターゲットに最適な差出人と文面を自動生成する。職員7741人のうち、ネット上に情報があったのは4010人で、このうち3310人に個人向けメールを送った。