— AUS（アルテミス・ユーザ・サポート）便り 2024/8/22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。

●8月14日リリースのWindows Update、IPv6の危険な脆弱性修正

https://forest.watch.impress.co.jp/docs/news/1615926.html
https://msrc.microsoft.com/blog/2024/08/202408-security-update/
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063

このニュースをザックリ言うと･･･

- 8月14日(日本時間)、マイクロソフト(以下・MS)より、Windows・Office等同社製品に対する月例のセキュリティアップデートがリリースされています。
- Windowsの最新バージョンはWindows 10 22H2 KB5041580(ビルド 19045.4780)および11 23H2 KB5041585(ビルド 22631.4037)となります。
- 今回、IPv6に関する特に危険度の高いとされる脆弱性(CVE-2024-38063)が修正されており、至急パッチを適用するよう呼び掛けられています。

AUS便りからの所感等

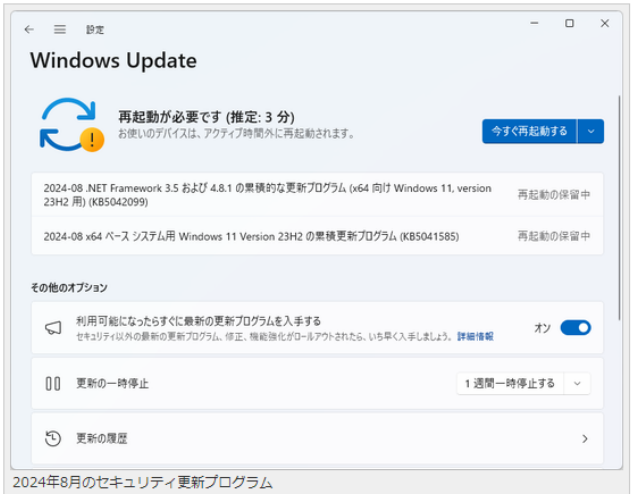
- IPv6の脆弱性は、細工したパケットを繰り返し送信することにより、PCやサーバーが乗っ取られる可能性があるとされています。
- Windows上でIPv6が有効でない場合は脆弱性の影響は受けないとされていますが、OSにおける設定方法の情報自体はMSのサイトに存在するとはいえ、現時点で今回の脆弱性の回避策としてその設定方法を明確に提示・推奨しているわけではないことには注意が必要です。
- 今回のセキュリティアップデートにおいてもこの他に危険度の高いものや既に悪用されているものも含めた多数の脆弱性が修正されており、前述したIPv6の脆弱性回避のために安易に緩和策をとって済ませるのではなく、根本的対策としてパッチの適用を行うことが肝要です。

Impress Watch

2024年8月の「Windows Update」～致命的・悪用の報告ありも含む90件の脆弱性に対処

できるだけ早い適用を

樽井 秀人　2024年8月14日 09:51



2024年8月のセキュリティ更新プログラム

米Microsoftは8月13日（現地時間）、すべてのサポート中バージョンのWindowsに対し月例のセキュリティ更新プログラムをリリースした（パッチチューズデー）。現在、「Windows Update」や「Windows Update カタログ」などから入手可能。Windows以外の製品も含め、今月のパッチではCVE番号ベースで90件の脆弱性が新たに対処されている。

●KADOKAWAグループへのランサムウェア攻撃で約25万人分の個人情報流出…ニコニコのアカウントは影響なし

https://www.itmedia.co.jp/news/articles/2408/05/news146.html
https://tp.kadokawa.co.jp/_assets/240805_release_f2A1q0nH.pdf
https://piyolog.hatenadiary.jp/entry/2024/08/19/074417

このニュースをザックリ言うと･･･

- 8月5日(日本時間)、KADOKAWA社およびグループ会社ドワンゴより、同社グループが6月上旬に受けたランサムウェア攻撃の結果、計254,241人分の個人情報が漏洩していたと発表されました。

- 個人情報が被害を受けたのは、ドワンゴ(全従業員)と同社の関係会社・取引先(クリエイター等含む)、N中等部・S高等学校・N高等学校(以下・N高)および運営する角川ドワンゴ学園とされています。

- 攻撃を受けた経路・方法は現時点で不明ながら、フィッシング等の攻撃によりドワンゴ従業員のアカウント情報が窃取されたことが根本原因であると推測、ここから社内ネットワークへの侵入、ランサムウェア感染に繋がったとしています。

- なお、ドワンゴ運営の「ニコニコ」各サービスについてはユーザーアカウントの流出は確認されておらず、グループ顧客のクレジットカード情報についても社内で保持していないため流出はなかったとのことです。

- 今回の攻撃については、セキュリティ研究者のpiyokango氏が8月19日に発表したブログ記事で詳細にまとめられています。

AUS便りからの所感

- 「ニコニコ動画」が復旧まで約2ヶ月を要し、他のサービスについても完全復旧は9月以降までかかるとされ、一部はデータが破壊されたことで復旧を断念したことも発表されたほか、ネット上のサービスのみならず出版事業や経理機能等にも影響が及んだとされています。

- KADOKAWAグループのデータセンターで運用されていたプライベートクラウドが侵入され、保存されていたデータが暗号化の被害を受けた一方、「ニコニコ動画」における一部システム・動画データ等が、攻撃の数か月前にAWSのパブリッククラウドに移行されており、たまたま被害を免れたものもあるとしています。

- KADOKAWA社からは今後も引き続き詳細な発表があるものとみられ、従業員アカウントの乗っ取り等があっても広範囲な被害の発生を阻止できるようなシステム構成の検討において一助となることを期待したいものです。

ITmedia NEWS

KADOKAWAサイバー攻撃、流出個人情報は25万人分　ニコニコユーザーは無事　端緒は従業員アカウントの漏えい

2024年08月05日 17時18分 公開　［岡田有花，ITmedia］

KADOKAWAは8月5日、6月上旬に受けた大規模なサイバー攻撃により漏えいした情報の詳細について、社外のセキュリティ企業よる調査結果を発表した。

漏えいした個人情報は25万4241人分で、ドワンゴの全従業員や一部の取引先、N中等部・N高等学校などの在校生・卒業生の一部などが含まれていた。「ニコニコ」ユーザーのアカウント情報の漏えいは確認していないという。

攻撃の標的は、ニコニコを中心としたサービス群。「フィッシングなどの攻撃により、従業員のアカウント情報が窃取され、社内ネットワークに侵入されたことで、ランサムウエアの実行と個人情報の漏えいにつながった」とみている。従業員のアカウント情報が窃取された経路や手法は「現時点では不明」としている。

● 7月度フィッシング報告は177,855件、9ヶ月ぶり最多更新

https://www.antiphishing.jp/report/monthly/202407.html

このニュースをザックリ言うと･･･

- 8月21日(日本時間)、フィッシング対策協議会より、7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。

- 7月度の報告件数は177,855件で、6月度(https://www.antiphishing.jp/report/monthly/202406.html)の144,160件から33,695件増加、過去最多を記録しています。

- フィッシングサイトのURL件数は38,591件で6月度(54,991件)から16,400件減少、悪用されたブランド件数は73件で6月度(71件)から2件増加となっています。

- ヤマト運輸を騙るフィッシングが全体の約30.6%を占め、次いで10,000件以上の報告を受けたAmazon、東京電力、三井住友カード、イオンカードと合わせて約82.6%、さらに1,000件以上報告された14ブランドまで含めると約97.1%を占めたとのことです。

AUS便りからの所感

- 報告件数は2024年3月以降右肩上がりが続き、これまで最多だった2023年10月度の156,804件よりも21,051件多くなっています。

- フィッシングサイトURLで使用されるTLD(トップレベルドメイン名)の割合は上位から .cn(約50.0%)、.com(約36.8%)、.net(約3.1%)、.dev(約2.8%)となっており、.cnが急増して半数を占めています。

- 日本語のフィッシングメールに関してはフィッシング対策協議会が特に警戒すべきものを取り上げている(https://www.antiphishing.jp/news/alert/)他、日本データ通信協会の迷惑メール相談センターからも日々10～20件のフィッシングメールが掲載されており(https://www.dekyo.or.jp/soudan/contents/news/alert.html)、不審なメールを受信した際はこういった情報との照合やソーシャルネットワークでの報告を確認するとともに、利用しているサービスのサイトへは事前に登録したブラウザーのブックマーク等からアクセスする等、慎重に行動することを日々心掛けてください。

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