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。

●新聞社系ECサイトにてクレジットカード情報流出発生…悪用も確認、被害額767万円

https://www.itmedia.co.jp/news/articles/2107/14/news116.html
https://yomifa.com/published_documents/index.html

このニュースをザックリ言うと･･･

- 7月14日(日本時間)、読売新聞グループの読売情報開発大阪社より、同社ECサイト「よみファネット」が不正アクセスを受け、クレジットカード情報が流出した可能性があると発表されました。

- 被害を受けたのは、2020年10月24日～2021年3月2日によみファネットに入力された1,301人分のクレジットカード情報(カード番号・名義人・有効期限およびセキュリティコード)となっています。

- 3月2日に決済代行事業者からの指摘を受けて当該サイトのサービスを全停止、4月12日に不正アクセスが発覚したとしており、既に58人分のカード情報が不正利用を受け、計7,674,605円の被害が出ていることが確認されているとのことです。

AUS便りからの所感等

- 今日における「ECサイトからのカード情報の流出」の事例では、サーバー上にカード情報を保存しない仕様が増えている状況を鑑み、「カード情報の入力フォームを改ざんし、入力されたカード情報を奪取する」手口へと主流が移行しています。

- 今回についても「不正アクセスにより決済処理プログラムの改ざんが行われた」のが流出の原因であると発表されており、フォームから入力されたクレジットカード情報が攻撃者にも送信される等に仕向けられた可能性が考えられます。

- そしてこのような改ざんに際しては、ECサイト構築で良く利用されるソフトウェアにおいて古いバージョンに存在する脆弱性が悪用されるケースが度々報告されていますので、根本的な対策として、使用している各ソフトウェアを常に最新のバージョンに保つこと、加えて不正なリクエストを検知・遮断するソリューションの導入や、外部機関による診断といった各種対策をとって頂ければ幸いです。

ITmedia NEWS

読売新聞子会社でクレカ情報流出　すでに767万円の金銭的被害も確認

2021年07月14日 14時39分 公開　[ITmedia]

印刷　736　Share　B!　67

読売新聞グループの読売情報開発大阪（大阪市）は7月14日、同社のECサイト「よみファネット」が不正アクセスを受け、1301人分のクレジットカード情報が漏えいした可能性があると発表した。一部の情報は不正利用され、少なくとも58人分のカード情報が不正利用を受け、計767万4605円の被害が出ていることを確認したという。

●モバイル回線専用アプリに不具合…別ユーザーの情報が表示

https://www.itmedia.co.jp/news/articles/2107/19/news070.html
https://www.iijmio.jp/info/iij/1626425153.html

このニュースをザックリ言うと・・・

- 7月15日(日本時間)、インターネットイニシアティブ社(以下・IIJ)より、同社「IIJmioモバイルサービス ギガプラン」専用アプリ「My IIJmio」に不具合があったと発表されました。

- My IIJmioは契約内容等の確認が可能なアプリで、同日午前10時にiOS・Android他向けに提供開始されたばかりでしたが、不具合により、アプリのログイン画面に入力されたID・メールアドレスのユーザーとは別のユーザーの情報(電話番号の一部・データ残量と有効期限・データ使用量・請求金額・および契約情報等)が表示される事故が発生し、午後18時55分にアプリの利用を停止したとしています。

- 同社では254名のユーザーが他のユーザーに情報が表示されたことを確認しており、個別にメールで連絡した上で、改修までサービスを停止することを発表しています。

AUS便りからの所感

- 不具合が発生した原因は後日詳細が発表されるとみられますが、ネット上の推測では、アプリの情報取得用サイトにCDNを使用した際にキャッシュ設定のミスがあり、あるユーザーに出力された情報がキャッシュされ、他のユーザーにも渡された可能性が指摘されています(この事例は2017年にメルカリで、2020年にソフトオンデマンドで発生が報告されています)。

- 別の原因による事例としては、2020年5月、雇用助成金オンライン申請において、同時刻に申請した申請者に同一のIDが割り振られたことによるもの(AUS便り 2020/06/08号参照)があります。

- Webサービスの構築にあたっては、こういった過去の事例について症状と発生原因に留意し、Webアプリケーション等においてくれぐれも他のユーザーの情報が渡されないような設計とするよう十分に注意してください。

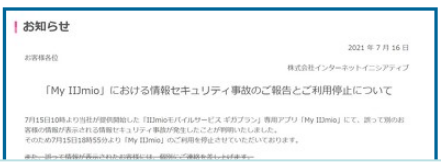
ITmedia NEWS

新アプリ「My IIJmio」で他人の情報誤表示　254人に影響

2021年07月19日 10時37分 公開　[ITmedia]

印刷　98　Share　B! 4

インターネットイニシアティブ（IIJ）は7月15日、同日午前10時に提供を始めたアプリ「My IIJmio」で、ログインページに入力したユーザーIDとは別のユーザーの情報が表示される事故が起きたため、午後6時55分からアプリの利用を停止したと発表した。


お知らせ

2021 年 7 月 16 日

株式会社インターネットイニシアティブ

「My IIJmio」における情報セキュリティ事故のご報告とご利用停止について

●Windowsの印刷機能に(複数の？)新たな脆弱性、悪意のあるプリンターへの接続で乗っ取りの恐れも

https://news.mynavi.jp/article/20210719-1925739/
https://pc.watch.impress.co.jp/docs/news/1339055.html

このニュースをザックリ言うと・・・

- 7月18日(現地時間)、米CERT/CCより、Windowsの印刷関連機能に脆弱性が存在するとして注意喚起が出されています。

- 脆弱性は、ターゲットとなるPCが外部の悪意のあるプリンターへ接続することにより、任意のコードをPC上で実行され、攻撃者によるPCの乗っ取り等が可能とされています。

- 前後して同15日には、マイクロソフト(以下・MS)より、Windowsの印刷スプーラー(Print Spooler)にローカルからPCの乗っ取りが可能な脆弱性「CVE-2021-34481」が存在すると発表されています。

AUS便りからの所感

- 両者が同一の脆弱性かは不明ですが、いずれも先日報告された「PrintNightmare」(AUS便り 2021/07/05号参照)とは別の脆弱性とみられ、かつPrintNightmareの対策が行われた7月の月例パッチではまだ修正されていないとみられます。

- CERT/CCが発表した脆弱性については、現時点で特筆すべき対策法はないとし、外部へのSMB(Windowsファイル共有等で使用されるプロトコル)通信を遮断する等の回避策をとるよう呼び掛けています。

- CVE-2021-34481の方も、先日のPrintNightmareと同様、MSより回避策として不必要な印刷スプーラーの実行を無効にすることが挙げられており、やはりパッチの適用と併せて、不必要なサービスの停止や、内部へのみならず外部との通信についても適宜遮断するようUTM等で設定を行うといった多重防御が肝要と言えます。

TECHI Powered by マイナビニュース

Windows、プリンタに接続するだけで管理者権限でコード実行の脆弱性

2021/07/19 12:17　著者：後藤大地

B!　URLをコピー

CERT Coordination Center (CERT/CC, Carnegie Mellon University)は7月18日(米国時間)、「VU#131152 - Microsoft Windows Print Spooler Point and Print allows installation of arbitrary queue-specific files」において、Microsoft Windowsにプリンタ関連の脆弱性が存在すると伝えた。この脆弱性を悪用されると、細工されたプリンタに接続することでSYSTEM権限で任意のコードが実行される危険性がある。