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。

●ソースネクストECサイトが不正アクセス…クレカ情報11万件漏洩か

https://www.itmedia.co.jp/news/articles/2302/14/news154.html
https://www.sourcenext.com/support/i/2023/0214_info/

このニュースをザックリ言うと･･･

- 2月14日(日本時間)、ソフトウェア販売大手のソースネクスト社より、同社ECサイトが不正アクセスを受け、クレジットカード情報を含む個人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、2022年11月15日～2023年1月17日にかけて当該サイトで商品を購入したユーザー最大120,982件分の個人情報(氏名・メールアドレス・住所・電話番号。パスワードは含まず)および112,132件分のクレジットカード情報(名義・番号・有効期限・セキュリティコード)とされています。
- サイトの脆弱性を悪用したペイメントアプリケーションの改ざんが流失の原因であるとしています。

AUS便りからの所感等

- 近年のECサイトからのクレジットカード情報漏洩ではセキュリティコードも含めての漏洩のケースが多く、サーバー上にカード情報を保持しない仕様であったとしても、フォームを改ざんすることにより、決済時に入力されたカード情報を外部に送信するような手口が主流となっています。
- ECサイト構築で利用される有名なフレームワークにおいて、SQLインジェクションの脆弱性が発見され、セキュリティアップデートが修正されたにも拘らず、それが適用されない状態のECサイトが攻撃を受けるケースも度々報告されています。
- 攻撃者による侵入や改ざんの余地をなくすため、Webアプリケーション・フレームワークからサーバーに至るまで最新のバージョンに保ち脆弱性の修正・対策を確実に行うよう心掛けるとともに、攻撃の形跡・兆候を検知・遮断するためのIDS・IPSおよびWAFの設置を行うことも検討するようにしてください。

ITmedia NEWS

ソースネクスト、最大で個人情報12万人分、カード情報11万人分漏えいの可能性　不正アクセス受け

2023年02月14日 16時45分 公開　[ITmedia]

ソースネクストは2月14日、同社ECサイトが不正アクセスを受け、最大で個人情報約12万人分、クレジットカード情報11万人分が漏えいした可能性があると明かした。脆弱性を悪用され、決済システムが改ざんされたのが原因としている。

(2)クレジットカード情報漏えいの可能性があるお客様

2022年11月15日～2023年1月17日の期間中に当サイトにおいてクレジットカード情報を登録されたお客様112,132名で、漏えいした可能性のある情報は以下のとおりです。

- カード名義人名
- クレジットカード番号
- 有効期限
- セキュリティコード

(3)個人情報漏えいの可能性があるお客様

2022年11月15日～2023年1月17日の期間中に当サイトにおいて購入されたお客様120,982名で、漏えいした可能性のある情報は以下のとおりです。

- 氏名
- メールアドレス（パスワードの漏えいはありません）
- 郵便番号（任意入力項目）
- 住所（任意入力項目）
- 電話番号（任意入力項目）

上記 (2)、(3)に該当するお客様については、別途、電子メールにて個別にご連絡申し上げます。

漏えいした可能性がある情報

漏えいした可能性がある情報は、ユーザーの氏名、メールアドレス、郵便番号、住所、電話番号など最大12万982人分とカード名義人名、クレジットカード番号、有効期限、セキュリティコードなどクレジットカード情報最大11万2132人分。2022年11月15日から23年1月17日の間にソースネクストで商品を購入したユーザーが対象。

●大学内のNASが外部からアクセス可能に→不正ログイン→ランサムウェア感染

https://scan.netsecurity.ne.jp/article/2023/02/14/48912.html
https://www.saitama-u.ac.jp/news_archives/2023-0207-1206-9.html

このニュースをザックリ言うと･･･

- 2月9日(日本時間)、埼玉大学より、業務で利用している複数のNASが不正アクセスを受け、データの一部がランサムウェアによって一時改変されたと発表されました。

- 不正アクセスを受けたのは2022年6月7日で、ネットワークアクセス制限の設定変更の不備が原因でNASが外部からアクセス可能になり、複数回のログイン試行で2台のNASがパスワードが破られて侵入、それを踏み台にして別の4台のNASにも侵入されたとしています。

- 同日のうちに外部からのアクセスは遮断され、データは復元済みとしています。

AUS便りからの所感

- NASや複合機等について、設定の不備で機器が外部からアクセス可能になるケースとしては、例えばUPnPが機器やルーターで有効になっていたことが原因での自動設定の問題が以前から取り上げられています。

- また、外部からアクセスされないことを前提にして、ネットワーク機器のパスワードをデフォルトから変えない、あるいは簡単なものとすることは、一たび同一LAN上に攻撃者が侵入した場合に容易に連鎖的な攻撃を受けることに繋がり得ます。

- ルーターが意図しない内部機器へのアクセスを許可しないよう確実に設定すること、各機器に推測されにくい十分に強力なパスワードを速やかに設定することがそれぞれ重要となります。

ScanNetSecurity

インシデント・事故／インシデント・情報漏えい

2023.2.14 Tue 8:05

埼玉大学のNAS4台にランサムウェア攻撃、データの一部が改変被害

国立大学法人埼玉大学は2月9日、同学の情報システムへの不正アクセスについて発表した。

シェア　ツイート　送る

国立大学法人埼玉大学は2月9日、同学の情報システムへの不正アクセスについて発表した。

トップページ

全２枚

拡大写真

これは2022年6月7日午前8時頃より、ネットワークアクセス制限の設定変更時の不備で学の業務で利用しているNASへの外部からのアクセスが可能となり、同日正午頃に攻撃者によるNASへの不正アクセスが開始され、複数回のログオン試行で2台のNASのパスワードが破られ、侵入したNASを経由して他の4台のNASへの不正アクセスが行われ、ランサムウェアによるデータの一部改変が行われたというもの。

●NEC製PCのプリインストール設定ツールに脆弱性…アップデートを

https://www.itmedia.co.jp/news/articles/2302/10/news186.html
https://jpn.nec.com/security-info/secinfo/nv23-001.html
https://jvn.jp/jp/JVN60320736/

このニュースをザックリ言うと･･･

- 2月10日(日本時間)、NEC社より、同社製PC用ツールに重大な脆弱性(CVE-2023-25011)が確認されたとして注意喚起が出されています(同日にはJPCERT/CC・IPAからも同じく注意喚起が出されています)。

- 脆弱性が存在するのは、同社製PC「Mate」「VersaPro」に工場出荷時にインストールされている「PC設定ツール」バージョン10.1.26.0およびそれ以前、「PC設定ツール2」バージョン11.0.22.0およびそれ以前で、脆弱性の悪用により、管理者権限でPCのレジストリが変更される恐れがあるとされています。

- 同社では脆弱性が修正された「PC設定ツール」バージョン10.1.27.0、「PC設定ツール2」バージョン11.0.23.0へのアップデートを呼び掛けています。

AUS便りからの所感

- PCに対してリモートから直接攻撃を行うよりも、メール等に添付された不正なプログラムを実行させることにより、脆弱性を悪用するケースの方が考えられます。

- 根本的な対策のために社内で管理している該当PCについてツールのアップデートを行うとともに、アンチウイルス・UTMにより、脆弱性を突こうとするマルウェアが実行される可能性を抑制することが肝要です。

ITmedia NEWS

影響度“高”　NECのビジネスPCに最初から入ってる「PC設定ツール」に脆弱性　対策は？

2023年02月10日 18時58分 公開　[ITmedia]

JPCERT/CCと情報処理推進機構（IPA）は2月10日、NECが提供する「PC設定ツール」に認証欠如の脆弱性があると報告した。同ツールはNEC製のPC（Mate/VersaPro）に工場出荷時点からインストールされているアプリケーションで、悪用されると管理者権限でレジストリを書き換えられる可能性があるとしている。

PC設定ツール

対象となる製品のバージョン

インストールされている「PC設定ツールLibrary」のバージョンが以下のシステム