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。

●フォームからの問合せ情報約7年分、不正アクセスで流出か

https://www.itmedia.co.jp/news/articles/2310/30/news149.html
https://www.bigmotor.co.jp/lib/news/news_list.php?id=703

このニュースをザックリ言うと･･･

- 10月30日(日本時間)、中古車売買のビッグモーター社より、同社Webサーバーが不正アクセスを受け、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、2016年11月～2023年8月にかけての問合せフォーム利用者の氏名・住所・電話番号・メールアドレス等とされています(件数未発表)。
- 8月18日に不正アクセスが発覚後、サーバー上に保管されている個人情報の削除と、当該フォームを含むWebサイトの一部を停止したとしています。

AUS便りからの所感等

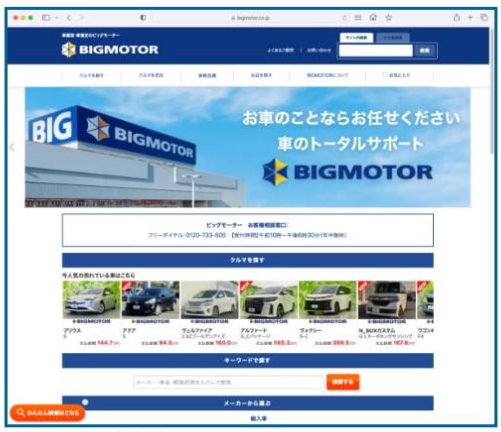
- クレジットカード情報・マイナンバー情報は収集しておらず、また顧客情報は別のシステムで保管しており、それぞれ流出はないとのことです。
- 流出した情報は問合せへの回答に必要な最低限の情報とみられますが、そのような必要に応じ収集し保有しているものについても、不要となり次第、適切にサーバー上等から破棄するようルールとシステムの整備を行うことは大切でしょう。
- この他、一般論とはなりますが、流出しては困るセンシティブな情報についてはできる限り最初から収集しないようにすること、万が一に不正アクセスが発生した際のデータの外部への流出を食い止めたり監視したりする出口対策を行うことも重要です。

ITmedia NEWS

ビッグモーターに不正アクセス、個人情報漏えいか　フォームからの問い合わせ、約7年分

2023年10月30日 17時30分 公開　[ITmedia]

中古車販売などを手がけるビッグモーター（東京都多摩市）は10月30日、自社Webサイトが第三者による不正アクセスを受け、「お問い合わせフォーム」から同社に連絡していた顧客の個人情報の一部が漏えいした可能性があると発表した。クレジットカード情報などは含まれていない。



ビッグモーターのWebサイト

同社によると、今年8月18日にWebサイトへの不正アクセスの痕跡を確認。該当するサーバーには、2016年11月から23年8月までにお問い合わせフォームを利用した人の住所、氏名、電話番号、メールアドレスなどの情報が含まれていた。クレカ情報やマイナンバー情報は収集していなかった。

●宛先を「Bcc:」以外に入力…メールアドレス流出相次ぐ

https://www.kek.jp/ja/notice/202311071100/
https://www.solize.com/news/2023/1102/
https://www.city.inuyama.aichi.jp/kurashi/community/1009832/1010150.html

このニュースをザックリ言うと･･･

- 11月7日(日本時間)、高エネルギー加速器研究機構(KEK)より、メール送信時の問題で、送信相手のメールアドレス1,315件が流出した可能性があると発表されました。

- 10月30日に関係者への情報提供のため、計4通のメールを一斉送信した際、メールアドレスをBcc: に入力するところ、誤って宛先欄(To: とみられる)に入力したとしています。

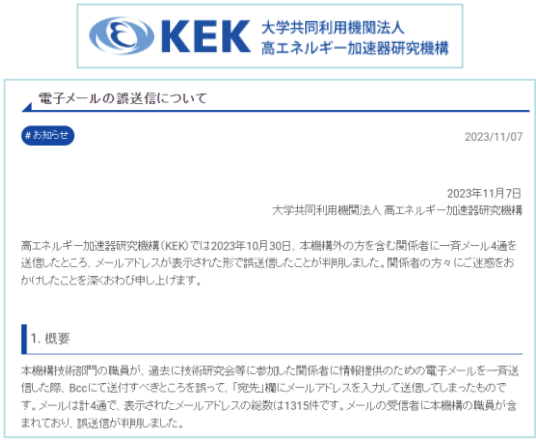
- 11月2日には3Dプリンティング等を手掛けるSOLIZE社より同様のミスでイベント参加者70件、同2日には犬山市からもセッション参加予定者11件のアドレス流出が発表されています。

AUS便りからの所感

- 再発防止策として、3組織では「宛先の厳密なチェック(ダブルチェック等)」を、加えてKEKは「Bcc: の原則使用禁止」「メーリングリストの活用」、SERIZE社も「メール配信システムの利用」を行うとしています。

- 数百件という多数のメールアドレスをメーラーのBcc: 欄にコピー＆ペーストしたり、ダブルチェック等を行ったりといった人力に依存するやり方は、ケアレスミスから流出に至ることを根本的に防止するものではなく、同報メール配信システムやメーリングリストの活用、メーラーで対応せざるを得ない場合はメーラー自身やアドオンの誤送信防止機能の使用、またメールサーバーやUTMにおける不審な大量送信時のチェック機構等があれば併せて使用するといった、システム側での対策を行うことを検討すべきです。

- ただし、システムによる対策においても、複雑な機構に潜むバグ(AUS便り2021/08/03号参照)であったり、有償サービスの更新忘れで機能しなくなる(同 2023/04/18号参照)ケースも報告されており、大量送信を想定したテスト等は不可欠でしょう。


KEK 大学共同利用機関法人 高エネルギー加速器研究機構

電子メールの誤送信について

お知らせ

2023/11/07

2023年11月7日
大学共同利用機関法人 高エネルギー加速器研究機構

高エネルギー加速器研究機構（KEK）では2023年10月30日、本機構外の方を含む関係者に一斉メール4通を送信したところ、メールアドレスが表示された形で誤送信したことが判明しました。関係者の方々にご迷惑をおかけしたことを深くおわび申し上げます。

1. 概要

本機構技術部門の職員が、過去に技術研究会等に参加した関係者に情報提供のための電子メールを一斉送信した際、Bccにて送付すべきところを誤って、「宛先」欄にメールアドレスを入力して送信してしまったものです。メールは計4通で、表示されたメールアドレスの総数は1315件です。メールの受信者に本機構の職員が含まれており、誤送信が判明しました。

●Windowsドライバーの脆弱性によるPC乗っ取りの可能性に注意喚起

https://news.mynavi.jp/techplus/article/20231106-2811370/
https://thehackernews.com/2023/11/researchers-find-34-windows-drivers.html
https://blogs.vmware.com/security/2023/10/hunting-vulnerable-kernel-drivers.html

このニュースをザックリ言うと･･･

- 11月2日(現地時間)、「The Hacker News」にて、Windowsのドライバーにデバイスの乗っ取りが可能な脆弱性が確認されたとする調査結果が取り上げられています。

- VMware傘下のセキュリティ研究企業であるVMWare Carbon Black社が10月31日に報告したもので、脆弱性を悪用することにより、権限を持たない攻撃者がファームウェアを消去・改変したり、OS上でより高い権限を取得する可能性があるとされています。

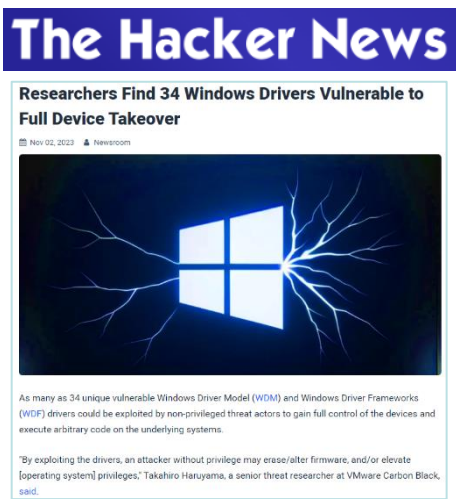
- IntelやAMDをはじめ、主要なチップ・BIOS・PCメーカー製を含む34のドライバーで、脆弱性が存在するとしています。

AUS便りからの所感

- 報告においては、Windows 11上の一般ユーザーが脆弱性を悪用するスクリプトを実行し、システム権限アカウントにログインしたり、ファームウェアを消去してPCが起動しないようにする等の実行例が掲載されています。

- ドライバーの脆弱性の悪用は、多くはリモートから直接ではなく、メールの添付ファイルやフィッシングサイト等からダウンロードした不正なプログラム・マルウェア等を巧妙に実行させる等の手口が考えられます。

- Windows Updateの実行のみではシステム上のドライバー全てが更新されるとは限らず、ドライバーを提供するベンダーによる独自のユーティリティ等によって最新に保つよう努めること、またマルウェア等のダウンロード・実行を防ぐためPC上でのアンチウイルスの有効化およびUTMによる防御が重要です。


The Hacker News

Researchers Find 34 Windows Drivers Vulnerable to Full Device Takeover

Nov 02, 2023 Newsroom

As many as 34 unique vulnerable Windows Driver Model (WDM) and Windows Driver Frameworks (WDF) drivers could be exploited by non-privileged threat actors to gain full control of the devices and execute arbitrary code on the underlying systems.

"By exploiting the drivers, an attacker without privilege may erase/alter firmware, and/or elevate [operating system] privileges," Takahiro Haruyama, a senior threat researcher at VMware Carbon Black, said.