— AUS（アルテミス・ユーザ・サポート）便り 2023/05/16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。

●クラウド環境の設定ミス…顧客情報約215万人分が10年近く公開状態に

https://www.itmedia.co.jp/news/articles/2305/12/news166.html
https://global.toyota/jp/newsroom/corporate/39174380.html

このニュースをザックリ言うと･･･

- 5月12日(日本時間)、トヨタ自動車より、グループ会社のトヨタコネクティッド社(以下・TC社)に管理を委託していたデータの一部が誤って外部に公開されていたと発表されました。

- 対象となるデータには2012年1月2日～2023年4月17日にT-Connect・G-Link・G-Link Lite・G-BOOKを契約した顧客約215万人分についての車両毎のIDや位置情報等が含まれており、外部に漏洩した可能性があるとされています。

- 2013年11月6日～2023年4月17日にかけて、クラウド環境の設定に誤りがあり、第三者からアクセス可能な状態にあったとのことです。

- この他、TC社の法人向けサービスから収集されたドライブレコーダーによる車外撮影映像についても、2016年11月14日～2023年4月4日にかけて同様に誤って外部からアクセス可能な状態にあったことが発表されています。

AUS便りからの所感等

- クラウド環境が何だったかの詳細は不明ですが、過去にはAmazon S3や、データベースサーバー「MongoDB」が外部からアクセス可能だったことによる情報流出の事例があり、今回も同様のものと推測されます。

- 同業他社の本田技研工業(Honda)で、2019年7月に分散処理型検索エンジン「Elasticsearch」のデータベースサーバーに設定ミスがあり、社内情報が外部からアクセス可能な状態にあったと発表されていましたが、このときにトヨタにおいても社内で同様の問題がなかったか点検していれば、より早期に発見・解決できていた可能性もあったとみられます。

- Webサーバーと連携するデータベースソフトウェア等については、同じホストで稼働している場合は外部からアクセスされないよう、また別々のホストで稼働している場合も不特定多数からの直接アクセスを遮断するよう、ホスト自身やルーター・UTMのファイアウォール機能で適切なアクセス制限を設定することが肝要です。

- これに加え(別のホストと連携する必要がある場合には特に)、パスワード設定によるアクセス保護を行うことは不可欠ですし、不正アクセスの有無やアクセス元等の分析のため、アクセスログを確実に取得する設定を行うこともまた強く推奨致します。

ITmedia NEWS

トヨタ「215万人分のクルマの位置情報、漏えいの可能性」公表　クラウド環境誤設定、約10年にわたり

2023年05月12日 16時02分 公開　[ITmedia]

トヨタ自動車は5月12日、同社のテレマティクスサービスに契約したユーザーのうち、215万人分の車両の位置情報・時刻が外部から閲覧された可能性があると発表した。

データ管理を委託した子会社・トヨタコネクテッドがクラウド環境を誤って設定し、約10年間にわたり、データが公開状態になっていたという。

また、トヨタコネクテッドは同日、法人向けサービスで収集した、ドライブレコーダーで車外を撮影した映像も閲覧された可能性があると発表した。

本日時点で把握している事案は以下のとおりです。

外部より閲覧された可能性があるお客様情報	車載端末ID*1、車台番号*2、車両の位置情報、時刻
対象となるお客様	2012年1月2日～2023年4月17日の期間内にT-Connect/G-Link/G-Link Lite/G-BOOKを契約されていた方(約215万人)
外部からアクセスできる状態にあった期間	2013年11月6日～2023年4月17日

*1車載機(ナビ端末)ごとの識別番号
*2車両一台ずつに割り当てられた識別番号

外部より閲覧された可能性がある情報	弊社が提供する法人向けサービスから収集されたドライブレコーダーで車外を撮影した映像
外部からアクセスできる状態にあった期間	2016年11月14日～2023年4月4日

トヨタコネクテッドのニュースリリースより

●WordPressプラグイン「MW WP Form」「Snow Monkey Forms」に脆弱性、アップデートを

https://jvn.jp/jp/JVN01093915/index.html
https://plugins.2inc.org/mw-wp-form/blog/2023/05/08/752/
https://snow-monkey.2inc.org/2023/04/28/snow-monkey-forms-v5-0-7/

このニュースをザックリ言うと･･･

- 5月8日(日本時間)、WordPressプラグイン「MW WP Form」「Snow Monkey Forms」の開発元より、各プラグインに脆弱性が確認されたと発表されました(5月15日にはIPA・JPCERT/CCからも注意喚起が出されています)。

- 脆弱性は「MW WP Form」バージョン4.4.2以前、「Snow Monkey Forms」バージョン5.0.6以前に存在し、悪用により、Webサーバー上への不正なファイルのアップロード・Webサイト改ざん・DoS攻撃・機微情報の窃取等が行われる可能性があるとされています。

- 脆弱性を修正した「MW WP Form」バージョン4.4.3(現在の最新は4.4.4)、「Snow Monkey Forms」バージョン5.0.7がリリースされています。

AUS便りからの所感


JVN#01093915
WordPress 用プラグイン MW WP Form および Snow Monkey Forms における複数の脆弱性

概要
株式会社モンキーレンチが提供する WordPress 用プラグイン MW WP Form および Snow Monkey Forms には、複数の脆弱性が存在します。

影響を受けるシステム
CVE-2023-28408、CVE-2023-28409
- MW WP Form v4.4.2 およびそれ以前のバージョン

CVE-2023-28413
- Snow Monkey Forms v5.0.6 およびそれ以前のバージョン

詳細情報
株式会社モンキーレンチが提供する WordPress 用プラグイン MW WP Form および Snow Monkey Forms には、次の複数の脆弱性が存在します。
- ディレクトリトラバーサル (CWE-22) - CVE-2023-28408
CVSS v3 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:L 基本値: 7.2
CVSS v2 AV:N/AC:L/Au:N/C:N/I:P/A:P 基本値: 6.4
- アップロードするファイルの検証が不十分 (CWE-434) - CVE-2023-28409
CVSS v3 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N 基本値: 5.3
CVSS v2 AV:N/AC:L/Au:N/C:N/I:P/A:N 基本値: 5.0
- ディレクトリトラバーサル (CWE-22) - CVE-2023-28413
CVSS v3 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L 基本値: 8.3
CVSS v2 AV:N/AC:L/Au:N/C:P/I:P/A:P 基本値: 7.5

- 「MW WP Form」は問合せフォーム作成のためのプラグイン、「Snow Monkey Forms」はその後継で、いずれも日本発のプラグインとして人気があります。

- 脆弱性にはいわゆる「ディレクトリトラバーサル」と言われるものが含まれており、Webアプリケーションが本来アクセスするディレクトリの外部にあるファイルの参照等が可能になる、古典的ながら危険度の高い脆弱性です。

- WordPress本体にも、機能拡張のため提供される数多くのプラグインにもしばしば脆弱性が報告されており、最初にサイトを構築してから、本体およびプラグインをアップデートしないままにしているのは非常に危険なため、管理者において定期的に管理画面へのログインを行い、本体・プラグインおよびテーマにおいてアップデートがリリースされていないか確認し、それぞれを最新バージョンに保つこと、またセキュリティ機能を提供するプラグインを導入することが肝要です。

●文化庁Web資料で漫画海賊版サイトへのリンク…マスク下の情報削除されず

https://www.sankei.com/article/20230516-MEHDOEVAR5NM3O44HQZX25FKJE/

このニュースをザックリ言うと･･･

- 5月16日(日本時間)、産経新聞より、「文化庁のサイトで、漫画をインターネット上に無断公開した海賊版サイトのURLが誤って半年以上、公開されていた」と報じられています。

- 2022年8月開催の教職員向け著作権講習会で使用された資料に、海賊版サイトへの日本国内からのアクセス上位10位に関するページが含まれており、サイト名とURLがマスクされていたものの、カーソルを合わせるとリンクが有効になっており、海賊版サイトにアクセス可能な状態となっていたとのことです。

- SNS上で話題になっていたとされ、同16日朝に当該資料は削除されたとのことです。

AUS便りからの所感

- Office文書(Word・Excel・PowerPoint)やPDF文書をWeb上で公開した際等に、非公開とすべき情報に黒塗り処理を行ったものの、隠れていた部分がコピー＆ペースト可能だったという事例は過去にも多数報告されています。

- マスキングされた箇所についてはその下の部分についてもテキストレベルからの修正・削除を行い、貼り付けられている画像へのマスクについても可能な限り画像データの方を修正して差し替えることが重要であり、またその状態でデータのコピー＆ペーストや検索(機密情報に繋がる入力へのマッチ)ができないかのチェックを行うべきです。

- 今回の事例では、講習会資料とはいえ、サイトのURL、ひいてはサイト名についても掲載すべきだったか疑問が残るところで、情報を不必要に公開・掲載しないことはそれだけでも十分なセキュリティ対策と言えます。

＜独自＞文化庁、漫画海賊版サイトを半年以上〝紹介〟 ＵＲＬ公開


海賊版サイト、日本国内からのアクセス 2022年7月 上位10サイト
(一社ABJ調べ/similarwebによる)

順位	サイト名	URL	2022年6月(単位=万)	2022年7月(単位=万)	6月→7月の増減率	態様
1	[redacted]	https:	3,243	3,754	115.8%	オンライン／ベトナム系
2		https:	106	3,686	3477.4%	オンライン／ベトナム系
3		http:/	3,585	3,410	95.1%	ダウンロード/リーチサイト
4		http:/	1,957	2,057	105.1%	ダウンロード/トレント
5		https:	1,746	1,614	92.4%	オンライン／(ベトナム系濃厚)
6		https:	2,050	1,524	74.3%	オンライン／ベトナム系
7		https:	1,034	1,485	143.6%	オンライン／ベトナム系
8		https:	979	1,064	108.7%	オンライン／ベトナム系
9		計測不能		626		オンライン／(ベトナム系濃厚)
10		https:	659	573	86.9%	オンライン／(ベトナム系濃厚)
		上位10サイト 合計	15,359	19,793	128.9%	1位・2位のアクセス数及び平均滞在時間が増加している(グレーマーカーは現在停止中)
		内 ベトナム系サイト 合計	7,412	11,513	155.3%	上位10サイトのうち5サイトがベトナム系サイトとなっている

文化庁のサイトに公開されていた漫画海賊版サイトの資料から。黒塗り部分にカーソルを合わせるとＵＲＬが表示され、海賊版サイトにアクセスできるようになっていた

文化庁のサイトで、漫画をインターネット上に無断公開した海賊版サイトのＵＲＬが誤って半年以上、公開されていたことが１６日分かった。著作権に関する講習会で使用した資料から海賊版サイトにアクセス可能な状態になっていた。ＳＮＳで話題になっているこ