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。

● ECサイトでカード情報流出相次ぐ…フォーム入力支援サービスに不正アクセス

https://www3.nhk.or.jp/shutoken-news/20221027/1000086213.html
https://www.showcase-tv.com/pressrelease/202210-fa-info/
https://www.abc-mart.net/shop/pages/info-2022.aspx
https://www.fujifilm.com/ffis/ja/news
https://www.kakuyasu.co.jp/corporate/topics/20221101.pdf

このニュースをザックリ言うと･･･

- 10月25日(日本時間)、Webマーケティング支援サービス等を提供するショーケース社より、同社サービスへの不正アクセスにより、複数のECサイトで情報漏洩が発生した可能性があると発表されました。

- 不正アクセスを受けたのは、入力フォーム支援サービス「フォームアシスト」、Webサイト表示最適化サービス「サイト・パーソナライザ」および「スマートフォン・コンバータ」で、サービスを利用する外部Webサイトに埋め込まれるソースコードが改ざんされたことが7月26日に指摘を受けて発覚したとのことです。

- 改ざんの影響により、ECサイトにおいてフォームに入力されたクレジットカード情報(カード番号・セキュリティコード等)の流出が相次いでおり、「ABCマート」で約2,300件、「富士フイルムイメージングシステムズ」2サイトでのべ1,370件、「カクヤス」で8,094件等とされています。

AUS便りからの所感等

- 多数の企業が利用するサービスが侵害され、機密情報の流出が発生した事例としては、2021年5月に発生した富士通製プロジェクト情報管理ツール「ProjectWEB」への不正アクセス(AUS便り 2021/08/24号参照)、またクレカ決済サービスではGMOペイメントゲートウェイ社への不正アクセス(AUS便り 2017/3/13号)等が挙げられます。

- ECサイト側が不正アクセスを受けたものではなく、サイトにアクセスしたユーザーに対し、改ざんされたプログラムはECサイトを経由せずに読み込まれる形となるため、このような攻撃をECサイト側で防御することは現時点では不可能に近いと思われます。

- ソフトウェア開発者のアカウントを乗っ取る等の行為により、配布物にマルウェアを混入させる「サプライチェーン攻撃」の一種とみることができ、ユーザー側(今回の事例ではECサイトとそれにアクセスするユーザー双方が該当します)で防御することは非常に困難な攻撃の一つとされており、今後発表されるであろう改ざんに至った不正アクセスの詳細を他山の石とし、組織内のシステムやアカウント管理の徹底を行うことにより、ユーザーが被害を受ける可能性を抑えることが肝要です。

NHK

ショッピングサイトのプログラム改ざん クレジット情報流出か

10月27日　15時28分

東京のＩＴ企業が開発し、複数のショッピングサイトなどで導入されている入力フォームのプログラムが何者かに改ざんされ、少なくとも３８００件以上のクレジットカードの情報が流出したおそれがあることがわかりました。

改ざんされたのは、東京・港区にあるＩＴ企業「ショーケース」が開発し、ショッピングサイトなどで導入されている入力フォームのサービスのプログラムです。
会社によりますと、ことし７月、取引先から指摘を受け、調査した結果、３種類のサービスのプログラムが外部からの不正アクセスによって改ざんされていたことがわかったということです。
これらのサービスは、さまざまなショッピングサイトなどに少なくとも５０００以上、導入されているということで、このうち一部のサイトで、入力された情報が外部に流出したおそれがあるとしています。

●OpenSSLバージョン3系に重大な脆弱性、至急アップデート適用を

https://news.mynavi.jp/techplus/article/20221027-2495790/

このニュースをザックリ言うと・・・

- 10月25日(日本時間・以下同様)、暗号化通信ライブラリ「OpenSSL」に重大な脆弱性が存在するとして、修正バージョンのリリースが予告されました。

- 脆弱性はOpenSSLバージョン3.0系に存在するとされ(1.1.1系およびそれ以前には存在しないとのことです)、2014年4月に修正された「Heartbleed」と同レベルに致命的なものとされています。

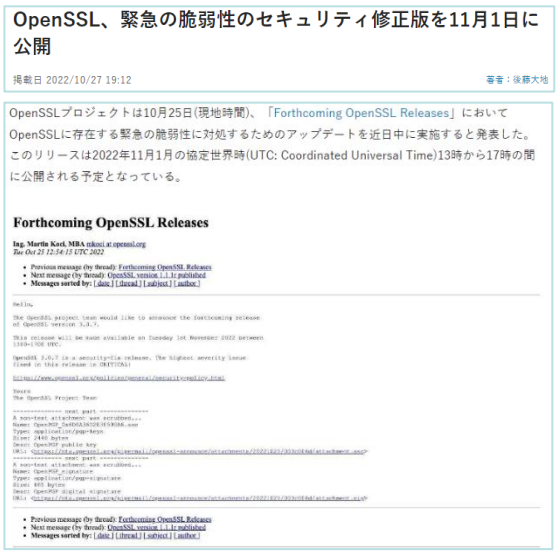
- 修正バージョン3.0.7は、11月1日夜間～同2日深夜にリリース予定とされ(追記：11月2日未明にリリースされました)、3.0系を利用している場合は速やかにアップデートが推奨されています。

AUS便りからの所感

- OpenSSLはHTTPSのみならずメール送受信やVPNといった広範囲なSSL/TLS暗号化通信等で使用され、脆弱性の内容によってはOpenSSLを使用するサーバー側・クライアント側両方が攻撃を受ける恐れがあります。

- 主なLinuxディストリビューションにおいては、AlmaLinux 9/Rocky Linux 9(その他RedHat Enterprise Linux 9をベースとしたバージョン)・Amazon Linux 2022やUbuntu 20.04LTSがOpenSSL 3.0系を使用しており、脆弱性の影響を受けるとされる一方、CentOS 7(RHEL 7)・AlmaLinux 8/Rocky Linux 8(その他RHEL 8ベース)・Debian 11およびUbuntu 20.04LTS以前は1.1.1系を使用しているため影響は受けない模様です(追記：11月2日時点でRHEL 9ベースおよびUbuntu 20.04LTSでは修正バージョンがリリースされています)。

- この他、OpenSSLを独自に組み込んでいるソフトウェア・アプライアンス等においても脆弱性の影響を受ける可能性があり、ベンダーからアップデートがリリースされる場合がありますので、更新情報を随時確認し、必要なアップデートがあれば即時適用できるような体制を整えることが重要です。


OpenSSL、緊急の脆弱性のセキュリティ修正版を11月1日に公開

掲載日 2022/10/27 19:12

OpenSSLプロジェクトは10月25日(現地時間)、「Forthcoming OpenSSL Releases」において OpenSSLに存在する緊急の脆弱性に対処するためのアップデートを近日中に実施すると発表した。 このリリースは2022年11月1月の協定世界時(UTC: Coordinated Universal Time)13時から17時の間に公開される予定となっている。

Forthcoming OpenSSL Releases

Hello,

The OpenSSL project team would like to announce the forthcoming release of OpenSSL version 3.0.7.

This release will be made available on Tuesday 1st November 2022 between 1300-1700 UTC.

OpenSSL 3.0.7 is a security-fix release. The highest severity issue fixed in this release is CRITICAL.

Yours,
The OpenSSL Project Team

●画像ソフト「GIMP」偽サイト、Googleの広告に出現か

https://gigazine.net/news/20221101-google-dangerous/

このニュースをザックリ言うと・・・

- 10月29日(日本時間)、ソーシャルニュースサイト「Reddit」において、画像ソフトウェア「GIMP」公式サイトの偽サイトがGoogle検索の上位に表示されたとする投稿がありました。

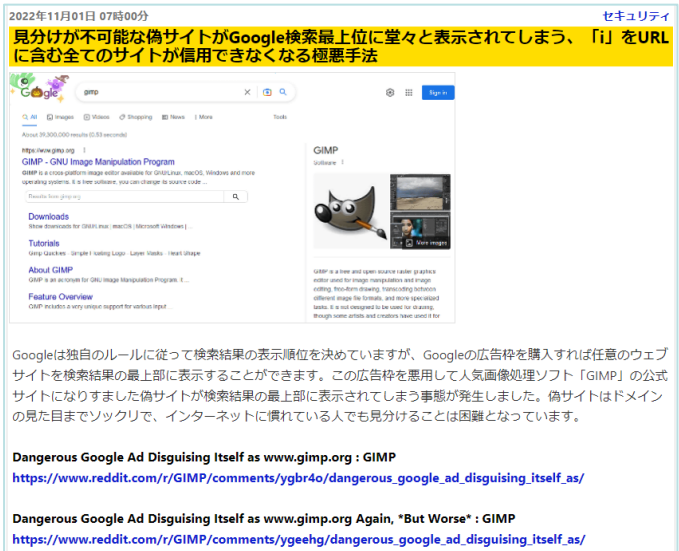
- 偽サイトは広告として表示され、トップページが本物の公式サイトと全く同じ外見ですが、ダウンロードボタンをクリックすると外部サイトから偽のインストーラーをダウンロードさせるものであったとされています。

- また、公式サイトのURLが「www.gimp.org」なのに対し、偽サイトは「i」の字がアルファベットではなくキリル文字の国際化ドメイン名(IDN)であった可能性が指摘されています。

AUS便りからの所感

- 先日も「えきねっと」の偽サイトがGoogle検索結果に広告として表示される事象が報告されたばかり(AUS便り2022/10/25号参照)ですが、今回はアルファベットと見間違えやすい文字を含む国際化ドメイン名を使うという(これも以前から頻繁に用いられている)手口と組み合わせたものとなっています。

- Googleをはじめとした大手サイト側には悪意のあるサイトを広告として表示しないよう、またWebブラウザー側にも悪用されやすい文字を含む国際化ドメイン名をそのまま表示しないようにするなどの対応が望まれますが、ユーザー側においてもこのような攻撃の手口があるということを念頭に置き、検索結果の上位、特に広告として表示されるサイトについて周辺の調査から安全かどうか判断すること等が重要です。


2022年11月01日 07時00分 セキュリティ

見分けが不可能な偽サイトがGoogle検索最上位に堂々と表示されてしまう、「i」をURLに含む全てのサイトが信用できなくなる極悪手法

Googleは独自のルールに従って検索結果の表示順位を決めていますが、Googleの広告枠を購入すれば任意のウェブサイトを検索結果の最上部に表示することができます。この広告枠を悪用して人気画像処理ソフト「GIMP」の公式サイトになりすました偽サイトが検索結果の最上部に表示されてしまう事態が発生しました。偽サイトはドメインの見た目までソックリで、インターネットに慣れている人でも見分けることは困難となっています。

Dangerous Google Ad Disguising Itself as www.gimp.org : GIMP
https://www.reddit.com/r/GIMP/comments/ygbr4o/dangerous_google_ad_disguising_itself_as/

Dangerous Google Ad Disguising Itself as www.gimp.org Again, *But Worse* : GIMP
https://www.reddit.com/r/GIMP/comments/ygeehg/dangerous_google_ad_disguising_itself_as/