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-CUBEの脆弱性突かれカード情報910件流出→WAF導入で阻止されていた

https://www.itmedia.co.jp/news/articles/2306/22/news204.html
https://www.city.shibushi.lg.jp/soshiki/5/22233.html

このニュースをザックリ言うと･･･

- 6月22日(日本時間)、鹿児島県志布志市より、同市の「ふるさと納税特設サイト」が不正アクセスを受け、クレジットカード情報が流出していたと発表されました。

- 被害を受けたのは、2021年3月12日～12月29日に同サイトでカード決済を行ったユーザー910件分のクレジットカード情報(番号・有効期限・セキュリティコード)およびWebサイトのログイン情報または電話番号(会員非登録者について)とされています。

- 不正アクセスが発覚したのは4月6日で、使用していたECサイト構築用ソフトウェア「EC-CUBE」の脆弱性を突かれたものとされている一方、2021年12月29日にWAFを導入して以降の情報流出は確認されていないとのことです。

AUS便りからの所感等

- 発表では、悪用されたのはクロスサイトスクリプティング(XSS)の脆弱性とされ、これにより、カード情報を窃取するためのプログラムを埋め込まれたとされています。

- 脆弱性が既にセキュリティアップデートが出ていたものか、それ以外のゼロデイの脆弱性なのかは現時点で明確ではありません(2021年6月にXSSの修正が行われていますが、これが該当するかは不明です)が、長期間アップデートを実施しておらず、脆弱性を悪用された情報流出に気付かないまま、WAFを導入した結果、たまたま流出を食い止めることに成功していた可能性があります。

- もちろん根本的な脆弱性への対策としてソフトウェアを最新バージョンに保つことが最も重要ですが、WAFやUTM等の導入による多重対策の検討は万が一の対策漏れを補完する目的では決して無意味なものではないでしょう。

ITmedia NEWS

志布志市ふるさと納税サイトでクレカ情報漏えいか　脆弱性突かれ不正プログラムを設置される

2023年06月22日 20時10分 公開　[ITmedia]

鹿児島県志布志市は6月22日、「志布志市ふるさと納税特設サイト」でクレジットカード情報910件が漏えいした可能性があるとして謝罪した。不正アクセスによりサーバに不正なプログラムを設置され、ユーザーがクレジットカード決済を実行した際にカード情報を盗み出すよう改造されたのが原因としている。

問題が発覚したのは4月6日。漏えいした可能性がある情報は2021年3月12日から12月29日までの間に同サイトでクレジットカード決済を行ったユーザーのクレジ

● Chromeに4件の脆弱性、セキュリティアップデート114.0.5735.198等適用を

https://forest.watch.impress.co.jp/docs/news/1511670.html
https://chromereleases.googleblog.com/2023/06/stable-channel-update-for-desktop_26.html

このニュースをザックリ言うと・・・

- 6月26日(現地時間)、Google社開発のChromeブラウザーにおいて、4件の重大な脆弱性(CVE-2023-3420, CVE-2023-3421, CVE-2023-3422他)が発表され、セキュリティアップデートがリリースされています。
- 脆弱性はJavaScriptエンジンやメディア処理部分等に存在し、悪意のあるWebサイトの閲覧等により、ブラウザーを実行しているPCを乗っ取られる恐れがあるとされています。
- Windows・Mac・Linux向けにセキュリティアップデート114.0.5735.198(およびWindows向けに114.0.5735.199)、Android向けに114.0.5735.196がリリースされており、インストールが強く推奨されます。

AUS便りからの所感

- Chromeと同じエンジンを使用する他のブラウザーにも同様の脆弱性が存在する可能性があり、例えばEdgeブラウザーにおいても今後セキュリティアップデートがリリースされる予定となっています(6月27日現在の最新バージョン114.0.1823.58は未対策とみられます)。
- ChromeではアップデートのAPI適用後に再起動を促すメッセージが表示されますが、リリースから適用・メッセージの表示までタイムラグが発生する場合があるため、「ヘルプ」→「Google Chromeについて」(もしくはchrome://settings/help)にて、最新バージョンへ確実にアップデートされているか確認する習慣をつけることが肝要です。

Impress Watch

「Google Chrome」に4件の脆弱性、最高深刻度は「High」

Windows環境にはv114.0.5735.198/199が、Mac/Linux環境にはv114.0.5735.198が順次展開

樽井 秀人　2023年6月27日 07:25

米Googleは6月26日（現地時間）、デスクトップ向け「Google Chrome」の安定（Stable）版をアップデートした。Windows環境にはv114.0.5735.198/199が、Mac/Linux環境にはv114.0.5735.198が順次展開される。

●日本郵政等サイト上の不審なスパムタイトルがGoogleに掲載…サイト検索の仕様を悪用か

https://togetter.com/li/2171158

このニュースをザックリ言うと・・・

- 6月19日(日本時間)頃、Googleで日本郵政のWebサイトを検索した結果に不審なタイトルのリンクが多数表示されるとTwitter上で報告がありました。
- タイトルの例として「最新情報を入手するには私のlineを追加」といったキーワードを含み、連絡先も記載されているものが挙げられているほか、他のサイト下でも同様のタイトルのリンクが表示されることも報告されています。
- Webサイトの検索機能を悪用し、不正なキーワードで検索した結果を第三者が検索エンジンに登録させる手口とされています。

AUS便りからの所感

- Webサイト側の検索機能の仕様により、「検索結果がなかった」場合でも、入力したキーワードがタイトルに表示される(そして検索エンジン上のリンクでもタイトルに使用される)、またそのページが「Not Found(コンテンツが存在しない)」として扱われないために検索エンジンに登録されてしまうことを、スパム業者等が悪用しているとされています。
- このような「検索結果がなかった」等のエラーページがGoogle等に登録されないようにするには、エラーページのステータスコードとして「200 OK」ではなく「404 Not Found」等を設定することが有用です。
- あるいは正当な検索結果があった場合等でも特定のページをGoogle等に登録されたくない場合は、検索エンジンが情報収集を行うボットへの動作指示として、robots.txtの設定あるいはHTML内に<meta name="robots" content="noindex">といったHTMLタグを埋め込む等を行うことを推奨致します。

togetter

トップ › 2023年 › 6月 › 20日

Googleで検索したら日本郵政のドメインの中にめちゃくちゃ怪しいタイトルが多数出てきたのだけどこれはどうやったんだろう?

怖いっすね

azu @azu_re
なんかめちゃくちゃ怪しいタイトルがsite:japanpost.jp で出てきた。これどうやったんだろ? pic.twitter.com/TXqMlHz292
2023-06-19 14:22:37

japanpost.jp
郵便番号 投資 信託 と は最新情報を入手するには私のlineを追加

これは怖い

seo-jizo（t.o） @jizo_seo
日本郵政がサイト内検索スパムの餌食に！？ twitter.com/azu_re/status/...
2023-06-20 09:26:35