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。

●Webアプリケーションフレームワーク「Spring Framework」に致命的な脆弱性「Spring4Shell」発見…至急アップデートを

https://internet.watch.impress.co.jp/docs/news/1399929.html
https://www.jpcert.or.jp/newsflash/2022040101.html
https://jvn.jp/vu/JVNVU94675398/index.html

このニュースをザックリ言うと･･･

- 3月31日(現地時間)、仮想マシンソフトウェアを提供するVMware社より、同社傘下で開発されているJava製のWebアプリケーションフレームワーク「Spring Framework」に重大な脆弱性(CVE-2022-22965)が存在すると発表されました(同日、JPCERT/CCおよびIPAからも相次いで注意喚起が出されています)。

- 「Spring4Shell」と名付けられた脆弱性は、Spring Framework バージョン5.3.0～5.3.17および5.2.0～5.2.19に存在し、悪用により、Webサーバー上で任意のコードが実行可能になり、サーバーの乗っ取り等に繋がる恐れがあるとされています。

- 発表時点で被害は確認されていないものの、脆弱性の有無を実証するコードが公開されているとのことです。

- 脆弱性を修正したバージョン5.3.18および5.2.20が同時にリリースされ、アップデートが強く推奨されています。

AUS便りからの所感等

- VMware社に報告された攻撃シナリオの成功には「JDK 9以降を使用」「Apache Tomcatをサーブレットコンテナとして使用」「WAR形式でデプロイ」「プログラムがspring-webmvcあるいはspring-webfluxに依存」といった条件を満たす必要があったとされていますが、該当する環境は決して少なくはないとみられ、また今後これらを満たさない場合にも悪用が可能となる攻撃コードが出回る可能性は十分に考えられます。

- 同じくJava上で動作するWebアプリケーションフレームワークとして一昔前に主流だったStrutsにおいても過去頻繁に脆弱性が報告され、これを悪用した攻撃による情報流出事故が度々発生していたのを鑑みれば、未対策のWebサイトは今この時点でも攻撃者によって探索され、攻撃を受ける恐れがあるため、根本的な対策として、Spring Frameworkを利用している全ての環境で速やかにセキュリティアップデートの適用が行われることが肝要です。

- 万が一アップデートが間に合わない、あるいは実行できない場合のみならず、今回Spring Frameworkを利用していなかったとしても、他のアプリケーションにおいて脆弱性が発見され、攻撃を受ける場面をもカバーできるよう、Webサーバーの前にWebアプリケーションファイアウォール(WAF)を設置することにより、不審なリクエストを遮断するよう防御することも、十分検討に値するでしょう。

Impress Watch

「Spring Framework」に深刻な脆弱性、「Spring4Shell」に対処したバージョンを公開

磯谷 智仁　2022年4月1日 19:36

Javaのウェブアプリ開発を行うためのフレームワーク「Spring Framework」に脆弱性（通称「Spring4Shell」）が確認されたとして、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）および脆弱性対策情報ポータルサイト「JVN（Japan Vulnerability Notes）」が情報を公開した。

Spring Frameworkには、データバインディングで使用する、CachedIntrospectionResultsクラス内のPropertyDescriptorオブジェクトの不適切な処理により、認証されていないリモートの攻撃者によって任意のJavaコードを実行される脆弱性（CVE-2022-22965）が存在する。その結果、遠隔の第三者によりclass.classLoaderを呼び出され、システム内で任意のJavaコードが実行される恐れがある。

● 3月度フィッシング報告件数は82,380件…過去最高を一気に更新

https://www.antiphishing.jp/report/monthly/202203.html

このニュースをザックリ言うと・・・

- 4月5日(日本時間)、フィッシング対策協議会より、3月に寄せられたフィッシング報告状況が発表されました。

- 3月度の報告件数は82,380件で、2月度(https://www.antiphishing.jp/report/monthly/202202.html)の48,611件から33,769件増加しており、またフィッシングサイトのURL件数は9,779件(2月度 7,547件)、悪用されたブランド件数も105件(2月度 87件)と急増、いずれも過去最高となっています。

- 報告全体に対するブランドの割合については、最も多いAmazonは約21.5%と割合・報告件数とも減少した一方、これとメルカリ、えきねっと(JR東日本)の3ブランドがそれぞれ10,000件以上報告され、併せて約55.0%を占める結果となった模様です。

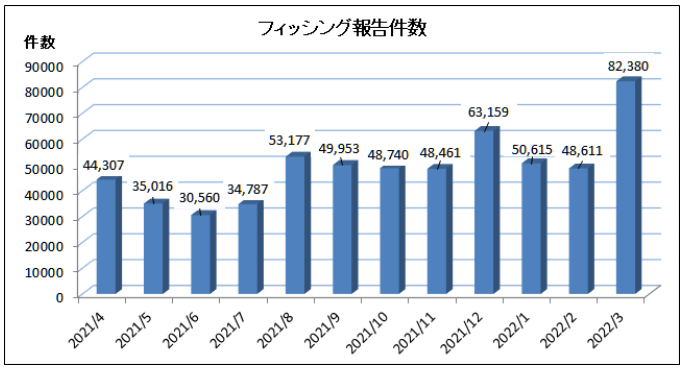
AUS便りからの所感

- ここ1年近くの報告件数に関しては、「急増による過去最高記録の更新」と「数か月間の落ち着き」とを繰り返しながら、徐々に高い水準で推移する傾向にあり、2021年1月度の43,972件から倍近くに増加しています。

- 同協議会からは3月4日に前述のえきねっとを騙るフィッシングについての注意喚起が出たのみならず、同18日にJR西日本の、同22日にはモバイルSuicaのフィッシングにも注意喚起が出される等、JRグループ系ブランドを騙るフィッシングも急増し、報告全体の割合も約21.1%に上ったとしています。

- この他、SMSによるフィッシング(スミッシング)から不正なAndroidアプリのインストールへ誘導するケース、Emotetへの感染を狙った添付ファイル付きメール等が今回も取り上げられた一方、受信検知・防止機構の一つであるSPFにより、調査用メールアドレス宛に届いたなりすましメールの約48.9%をhardfail(送信元認証に失敗)として検出する等の効果があったことも取り上げられており、あらゆる組織のメールサーバーにおいて、SPF(およびDMARC・BIMI)といった機構の導入が引き続き検討されるべきでしょう。

フィッシング対策協議会
Council of Anti-Phishing Japan



●デジタル庁からのメール、アドレス5件が他者に表示…昨年11月にも同様の事故

https://www.itmedia.co.jp/news/articles/2204/01/news166.html
https://www.digital.go.jp/press/a9874a8b-c99e-495f-8117-2f342403153b/

このニュースをザックリ言うと・・・

- 4月1日(日本時間)、デジタル庁より、メール送信時にミスがあり、メールアドレスが他者に流出する事象が発生していたと発表されました。

- 同庁が運用する新型コロナウイルス接種証明書アプリのヘルプデスクへの問合せに対する返信の際、送信されたメールには表示されない「Bcc:」に記載すべきメールアドレス5件を誤って「To:」に記載したことにより、メール受信者がこれらのメールアドレスを読み取ることが可能な状態となっていたとのことです。

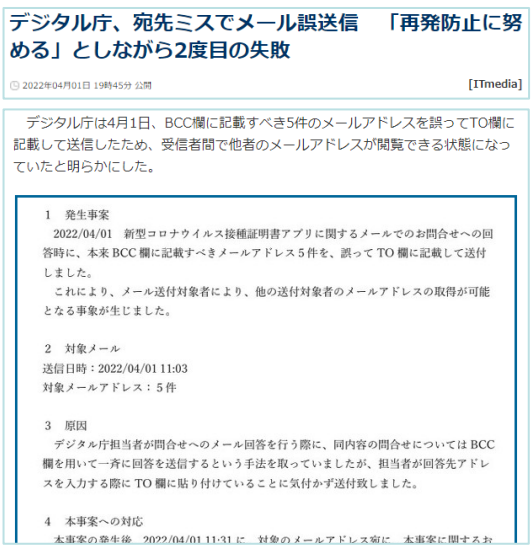
AUS便りからの所感

- 同庁では昨年11月にも、プレスリリース送信時にメールアドレス約400件を「Bcc:」ではなく「Cc:」に記載したことによる流出事故が発生していました(AUS便り 2021/11/30号 参照)。

- 今回においても、問合せへの返信を行うたびに、毎回複数のメールアドレスをその都度メーラーのBcc:に入力する形がとられていたとみられ、一度に入力されたアドレスの数あるいはこれを実行する頻度次第で(さらには「大量のアドレスを複数回に分けて入力する」ケース等の場合)、ミスが発生するリスクやミス発生時の被害は大きいものとなり得ます。

- 再発防止策として「メール送信時の宛先設定の確認を徹底する」としていますが、メーラーのみを用いて単なる目視チェック・複数人チェック等で事故を防止するのではなく、問合せ者と関係者それぞれに適切にメールを送信するためのシステム構築やメール配信サービス等の利用、また長大なTo:やCc:ヘッダーを含むメールをUTM等で遮断・警告を返すような仕組みの採用、あるいはメーラーにおいてもそれ自身やアドオンによる誤送信防止機能の活用等、機械的な予防策の導入が重要です。

ITmedia NEWS



デジタル庁、宛先ミスでメール誤送信　「再発防止に努める」としながら2度目の失敗

2022年04月01日 19時45分 公開　[ITmedia]

デジタル庁は4月1日、BCC欄に記載すべき5件のメールアドレスを誤ってTO欄に記載して送信したため、受信者間で他者のメールアドレスが閲覧できる状態になっていたと明らかにした。

1　発生事案
2022/04/01　新型コロナウイルス接種証明書アプリに関するメールでのお問合せへの回答時に、本来 BCC 欄に記載すべきメールアドレス 5 件を、誤って TO 欄に記載して送付しました。
これにより、メール送付対象者により、他の送付対象者のメールアドレスの取得が可能となる事象が生じました。

2　対象メール
送信日時：2022/04/01 11:03
対象メールアドレス：5 件

3　原因
デジタル庁担当者が問合せへのメール回答を行う際に、同内容の問合せについては BCC 欄を用いて一斉に回答を送信するという手法を取っていましたが、担当者が回答先アドレスを入力する際に TO 欄に貼り付けていることに気付かず送付致しました。

4　本事案への対応
本事案の発生後、2022/04/01 11:31 に、対象のメールアドレス宛に、本事案に関するお