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。

●企業向け広報サービス、発表前情報に関するファイルが第三者に取得される

https://www.itmedia.co.jp/news/articles/2107/09/news145.html
https://www.itmedia.co.jp/news/articles/2109/22/news154.html
https://prtimes.jp/common/file/20210709_PRTIMES_incident.pdf
https://www.release.tdnet.info/inbs/140120210922400852.pdf

このニュースをザックリ言うと・・・

- 7月9日(日本時間)、プレスリリース配信サイト「PR TIMES」の運営元より、同サイト上にある発表前の情報に関する一部ファイルが第三者に不正に取得されたと発表されました。

- その後9月22日に発表された調査結果によれば、不正に取得された可能性があるのは、2020年11月13日～2021年7月6日にかけて、同サイト会員企業16社のプレスリリース871件に紐づく画像のzipファイル866点、PDFファイル91点とされています。

- 機能面でのセキュリティホールが原因で不正取得が可能になったとしており、7月6日に修正を行って以降は発表前情報に関するファイルの不正取得は確認されていないとのことです。

AUS便りからの所感等

- セキュリティホールの内容は、画像のzipファイルおよびPDFファイルをダウンロードする機能において、ファイルにアクセスするためのURLが第三者から推測しやすいものになっていた、というものであり、例えばWebサイト等にログインする際のパスワードでもそうですが、第三者から悪用されないための前提を担保するのは、長さと複雑さの両方が十分な文字列となります。

- Webアプリケーション等を開発するためのプログラミング言語では大抵セキュリティに配慮した乱数を生成する仕組み等が用意されているため、日時をベースとする等自前で安易なロジックを作ることなく、そういった仕組みの存在をあらかじめ調査し、利用するよう心掛けることが、安全なWebアプリケーションをはじめとしたシステム開発においては肝要です。

- また、本来発表前の情報に関するファイルがログイン中のユーザーからのみ参照可能な状態か、等を確認するため、第三者機関によるセキュリティ診断を随時受けることや、第三者が不正にファイルを取得しようとする不審なアクセスを検知・遮断できるようなソリューションの導入も適宜検討することを推奨致します。

ITmedia NEWS

企業向け広報サービス「PR TIMES」で新たな情報漏えい明らかに　発表前の情報含む699件

2021年09月22日 19時53分 公開　[荒岡瑛一郎，ITmedia]

印刷　235　Share　B! 27

会員企業の報道資料を配信するサービス「PR TIMES」で、当時未発表だった画像ファイルなどを誤って公開してしまった問題で、運営元のPR TIMES社（東京都港区）は9月22日、新たに699件のファイルが取得されていたと発表した。7月の発表当初は258件と発表していた。

追加の調査を行ったところ、2020年11月13日～21年7月6日に配信した発表内容に添付する画像をまとめたZIPファイル636点と、発表文などが書かれたドキュメントファイル66点が取得されていたと新たに分かった。インサイダー情報の流出は確認していないという。

●Miraiの3倍以上の攻撃、新しいDDoSボットネット「Meris」8月に発生

https://www.itmedia.co.jp/news/articles/2109/24/news041.html
https://blog.cloudflare.com/cloudflare-thwarts-17-2m-rps-ddos-attack-the-largest-ever-reported/

このニュースをザックリ言うと・・・

- 9月24日(日本時間)、ITmedia NEWSにおいて、新たなボットネット型マルウェア「Meris」が8月に行った過去最大規模のDDoS攻撃について取り上げられています。

- 8月19日(現地時間)のCDN大手Cloudflare社からの発表によれば、同社顧客の金融機関がMerisによるとみられる毎秒1,720万回の不正なリクエストを受けており、これまで最大だったDDoS攻撃のほぼ3倍に上ったなどとしています。

- Cloudflareではこの攻撃については事前に検知して食い止められたものの、その数週間前にも同じボットネットから別の顧客に対し攻撃があったとしています。

AUS便りからの所感

- 9月以降もMerisによる攻撃は続いている模様で、9月5日にはロシア大手IT企業のYandex社が、同9日にも著名なセキュリティ研究者のWebサイトが攻撃を受けたとしています。

- Merisの名付け親となったDDoS対策企業Qrator社によれば、Merisの浮上が確認されたのは6月にさかのぼり、ラトビアのIoT機器メーカーMikroTik製のルーターの脆弱性を突いて侵入し、ボットネットを構築していたとのことです。

- 今後Miraiと同様様々なメーカー製のIoT機器へ侵入する恐れが考えられるため、管理画面等へアクセスするためのポートに外部から、あるいは社内の任意のネットワークからアクセスできないよう、UTM等を用いた安全なネットワークとなっているか確認することが重要です。

ITmedia NEWS

新手の「疫病」ボットネットが仕掛ける大規模DDoS攻撃、威力はMiraiの3倍以上

2021年09月24日 08時00分 公開　[鈴木聖子，ITmedia]

印刷　通知　118　Share　B! 8

世界各地で8月から9月にかけ、過去最大級のサイバー攻撃が相次いで発生した。中でも、標的に大量のトラフィックを送り付けてサービス不能状態に陥れるDDoS攻撃は、新手のボットネット「Meris」に操られた25万台のルーターから仕掛けられたという。その威力は、5年前に猛威を振るったIoTマルウェア「Mirai」の3倍を超えていた。

●Let's Encryptの古いルート証明書、9月いっぱいで期限切れ…古いデバイス・ソフトウェアに影響

https://news.mynavi.jp/article/20210922-1978106/
https://jp.techcrunch.com/2021/09/25/2021-09-21-lets-encrypt-root-expiry/
https://scotthelme.co.uk/lets-encrypt-old-root-expiration/

このニュースをザックリ言うと・・・

- 9月21日(現地時間)、イギリスのセキュリティ研究者Scott Helme氏より、無料でSSL証明書を発行するサービス「Let's Encrypt」が以前使用していた古いルート証明書(DST Root CA X3)が9月30日をもって有効期限が切れることについて注意喚起が出されています。

- Let's Encryptが現在発行する証明書は既に新しいルート証明書(ISRG Root X1)が参照される形に切り替えられていますが、以前使われていたルート証明書の方しか入っていない古いOSやアプリケーションの場合、Webサーバー等の証明書を適切に検証できず、信頼できないとみなす可能性があり、何らかの問題が発生し得るとされています。

- 問題が発生するOS・アプリケーション(およびバージョン)としては、Windows XP・macOS(10.12.1よりも前)・iOS(10よりも前)・Firefox(50よりも前)・OpenSSL(1.1.0よりも前)等が挙げられています。

- Android(7.1.1よりも前)についても新しいルート証明書が入っていませんが、依然該当するバージョンが広く利用されていることを鑑み、2024年初頭までは問題が回避されるよう、Let's Encrypt側で対応が行われています。

AUS便りからの所感

- 古いOS等で発生し得る問題としては、Web閲覧時に警告が表示されるようになる等が考えられますが、自動的に外部のWebサーバーにアクセスして情報を取得する等を行うプログラムが正常に動作しなくなる恐れもある点には注意が必要です。

- 古いバージョンのOS・アプリケーションを使い続けることは、この他にもサポート切れにより脆弱性が修正されなくなる等の事態も生じ、攻撃者やマルウェアの侵入を許すなどの事態に陥る恐れもありますので、PCやモバイル、サーバーやクライアントの区別なく、あらゆるデバイスについて可能な限り最新のバージョンに保たれているよう管理する体制を整えることが肝要です。

TECHR Powered by マイナビニュース

9月末でLet's Encryptルート証明書が期限切れ、古い製品は要注意

2021/09/22 08:12　著者：後藤大地

B!　URLをコピー

人気の高いSSL証明書認証局であるLet's Encryptが使っているルート証明書の有効期限が近づいている。「IdentTrust DST Root CA X3」で認識されるこのルート証明書の有効期限は2021年9月30日、つまり今月いっぱいまでだ。古いルート証明書から新しいルート証明書への移行は完全に透過的だが、実際には過去に問題が発生している。特に古いソフトウェアを使っている場合は注意が必要だ。